Release Notes

Dell Management Console

for Dell Enterprise Mobility Management and Dell Wyse Cloud Client Management

March 5, 2014

Copyright Notices

Copyright © 2014, Dell Inc. All rights reserved.

This manual and the software and firmware described in it are copyrighted. You may not reproduce, transmit, transcribe, store in a retrieval system, or translate into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, any part of this publication without express written permission.

Table of Contents

"R5a" Release (March 5, 2014) 4
- Release Overview 4
- New Features Details 4

"R5" Release (February 6, 2014) 7
- Release Overview 7
- New Features Details 7
- Supported Devices 11
- Known Issues 14
- Issues resolved in this release 14

"R4" Release (December 8, 2013) 16
- Release Overview 16
- New Features Details 18
- Supported Devices 33
- Known Issues 36
- Issues resolved in this release 36

"R3" Release (October 10, 2013) 37
- Release Overview 37
- New Features Details 38
- Supported Devices 51
- Known Issues 53
- Issues resolved in this release 53

"R2A" Release (August 16, 2013) 54
- Release Overview 54
- New Features Details 55
- Supported Devices 64

"R2" Release (June 28, 2013) 66
- Release Overview 66
- New Features Details 66
- Supported Devices 74
- Known Issues 75
- Issues resolved in this release 76

"R1" Release (May 24, 2013) 77
- Release Overview 77
- New Features Details 77

- Supported Devices 90
- Upgrade Notes 91
- Known Issues 92

"R5a" Release (March 5, 2014)

- **Release Overview**

The "R5a" release includes rebranding of the Cloud Client Manager platform – the Cloud Client Manager server has been renamed to Dell Management Console. This release also supports the new Dell Mobile Workspace solution. The server and device agent names and colors have been updated to reflect the changes in branding.

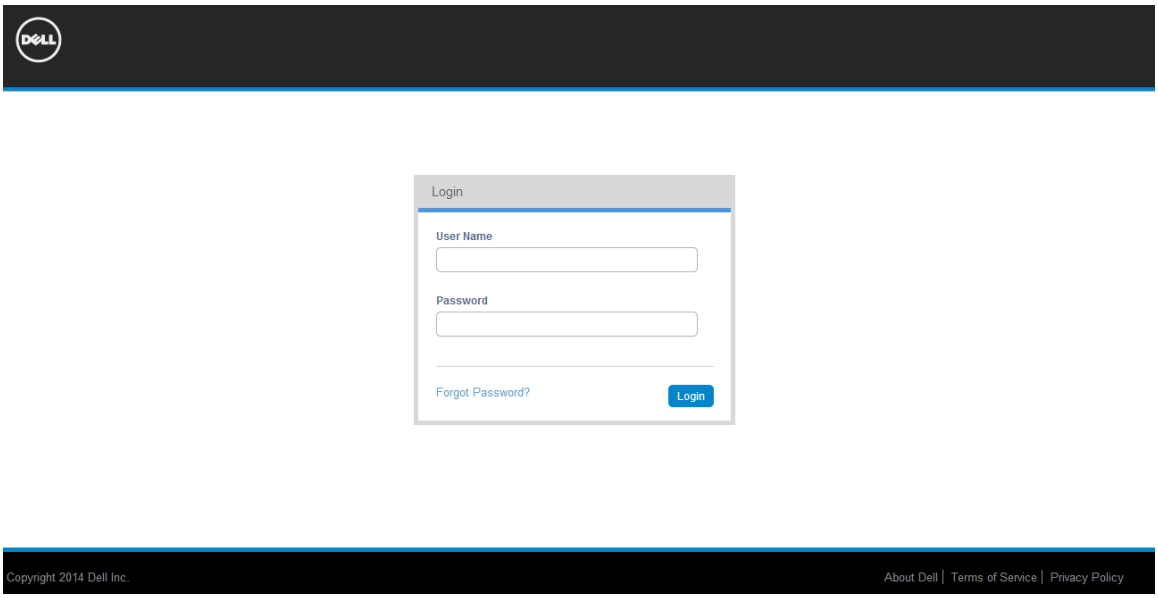
Some of the highlights of this release:

- New name: "Cloud Client Manager" is now "Dell Management Console"
- New name: "Cloud Client Manager Agent" is now "Dell Mobile Management Agent"
- New name: "CCM On Premises Gateway" is now "Dell On Premises Gateway"
- Updated Android Agent branding
- Updated iOS Agent branding
- Updated the CCM icons/colors to Dell icons/colors
- Support for Dell Mobile Workspace: Available for iOS and Android devices, enablement of a secure container for accessing corporate content and resources. For further details visit: http://software.dell.com/products/container-management-for-mobile-devices/

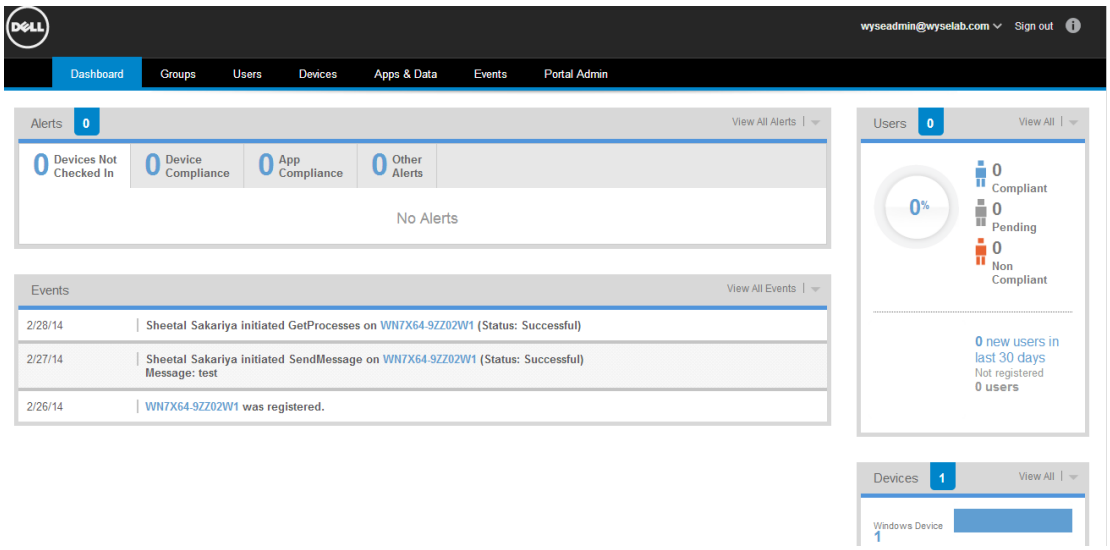
- **New Features Details**

1. **Details on the renaming/icons/rebranding of Cloud Client manager:**

   a. "**Cloud Client Manager**" name has been removed from top of page.



b. Cloud Client Manager icons have been replaced with Dell branded icons/colors.



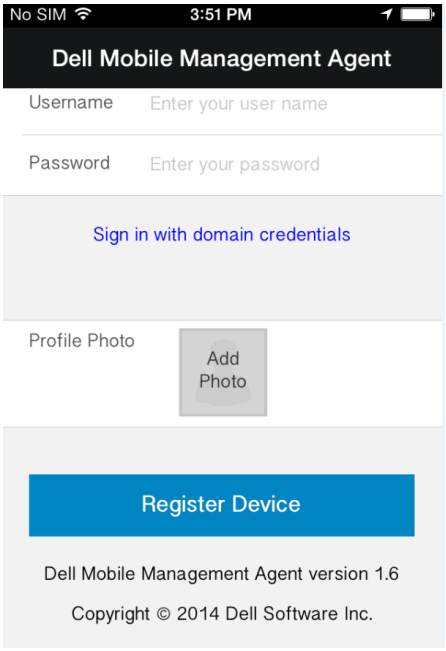
c. Rebranded “Cloud Client Manager Agent” is now “Dell Mobile Management Agent.” The Dell icon that will appear on the agent side is below.

Old icon:

New icon:

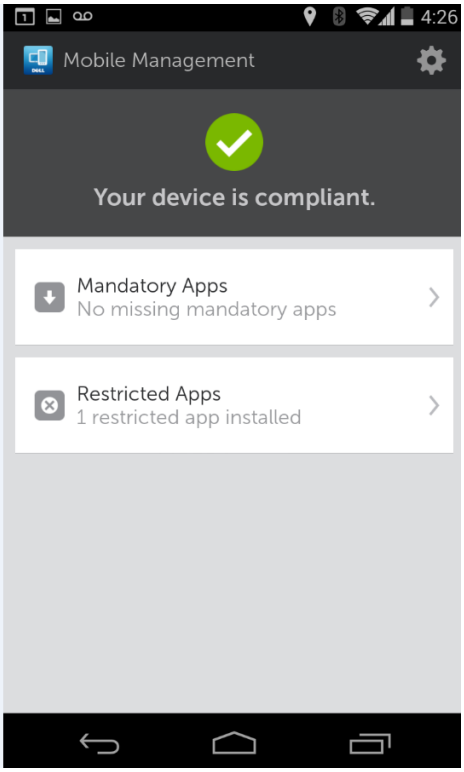
d.

For iOS agent, in addition to icon and **Dell Mobile Management Agent** app name changes, the colors in the app have been updated and the header is now “**Dell Mobile Management Agent**”. Also, replaced "**Sign in with Cloud Client Manager Account**" text with "**Sign in with Dell management portal account**" (from SSO sign-in page).

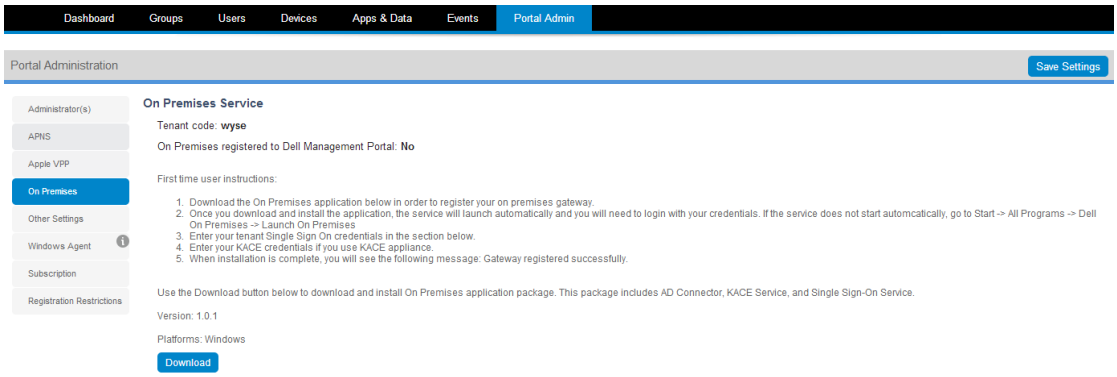


e.

For Android agent, in addition to icon and Dell Mobile Management Agent app name changes, the header is now “**Dell Mobile Management Agent**”. Also, replaced "**Sign in with Cloud Client Manager Account**" text to "**Sign in with Dell management portal account**" (from SSO sign-in page).



f. The On Premises name has changed from **Cloud Client manager On Premises** to **Dell On Premises Gateway** as shown below in the image.


Dashboard
Groups
Users
Devices
Apps & Data
Events
Portal Admin
Portal Administration
Save Settings
Administrator(s)
APNS
Apple VPP
On Premises
Other Settings
Windows Agent
Subscription
Registration Restrictions
On Premises Service
Tenant code: wyse
On Premises registered to Dell Management Portal: No
First time user instructions:
1. Download the On Premises application below in order to register your on premises gateway.
2. Once you download and install the application, the service will launch automatically and you will need to login with your credentials. If the service does not start automcatically, go to Start -> All Programs -> Dell On Premises -> Launch On Premises
3. Enter your tenant Single Sign On credentials in the section below.
4. Enter your KACE credentials if you use KACE appliance.
5. When installation is complete, you will see the following message: Gateway registered successfully.
Use the Download button below to download and install On Premises application package. This package includes AD Connector, KACE Service, and Single Sign-On Service.
Version: 1.0.1
Platforms: Windows
Download

"R5" Release (February 6, 2014)

- **Release Overview**

The Cloud Client Manager "R5" release includes new functionality for both the platform and for device management on all device types.

Some of the highlights of this release:

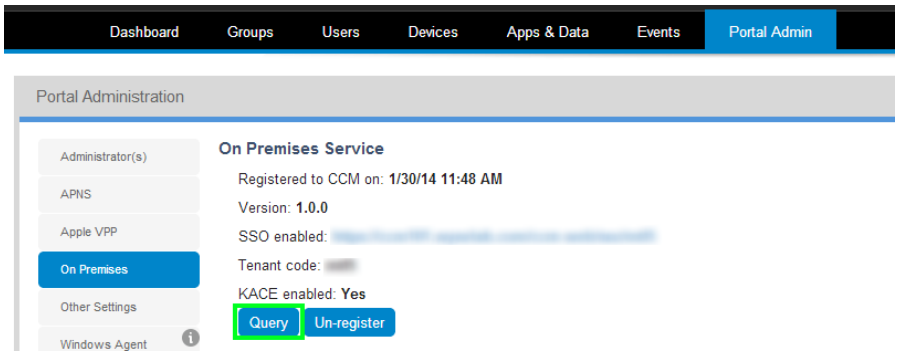
- **On Premises Gateway Management Enhancements:**
  - New option to validate from CCM console the On-Premises Gateway configured URL
  - New option to remotely Unregister On-Premises Gateway (and 'Force Unregister' if gateway is no longer reachable)
  - Display Tenant Code and SSO login link in the Portal Admin -> On Premises page to simplify Single Sign-On user experience
  - New option to manually trigger export of mobile device asset inventory into Dell KACE K1000 appliance
- **Other Platform Enhancements:**
  - Improved messaging for iOS device registration for missing/expired MDM APNS certificates
  - Display last connection and security settings status in System Status section of Windows Devices
  - Support for CCM console Administrators to update their own login name
  - Dell Mobile Workspace support

- **New Features Details**

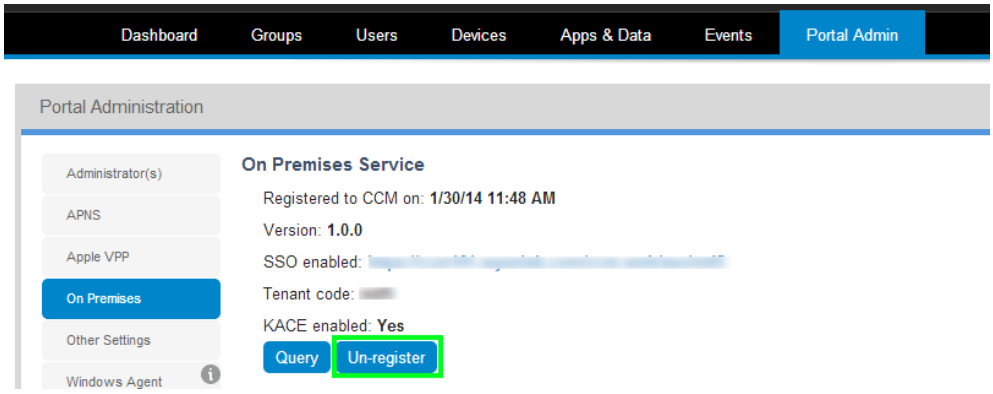
g. **<u>On Premises Gateway Management Enhancements</u>**

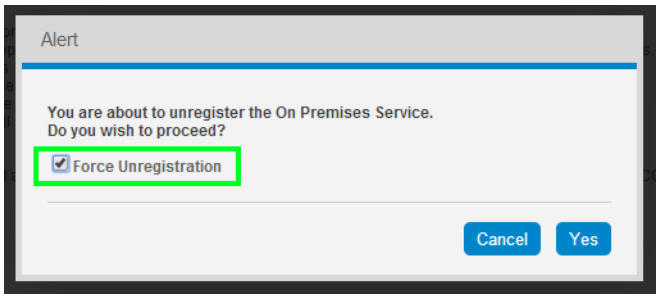
Available from **Portal Admin > On Premises**, new functionality available to improve the **On Premises Gateway** functionality.

a. **Validate On-Premises Gateway configured URL**: Click the "**Query**" button to validate that the CCM server can access the registered On Premises Gateway. If able to reach the remote gateway, then a new tab will open with the message "Succesful!".

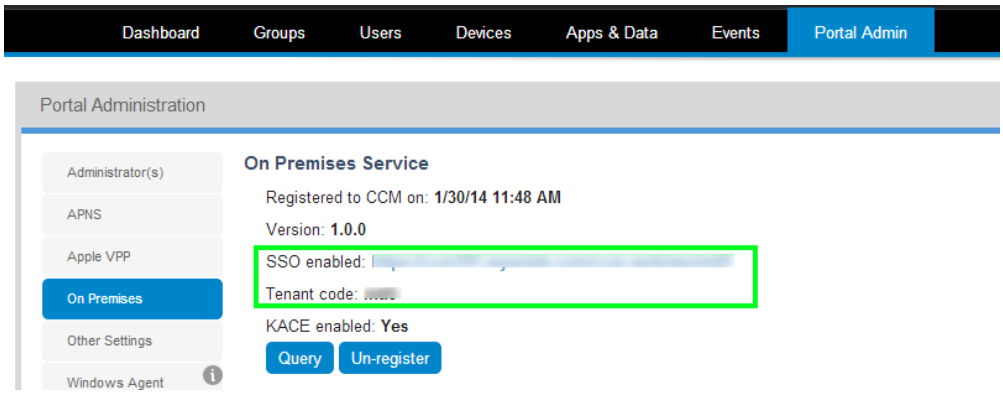


b. **Remotely Unregister (& 'Force Unregister') On Premises Gateway**: Click the "**Un-register**" button to unregister the currently registered On Premises Gateway. If the On Premises Gateway is no longer reachable use the "**Force Unregistration**" checkbox to forcefully unregister the gateway from CCM.

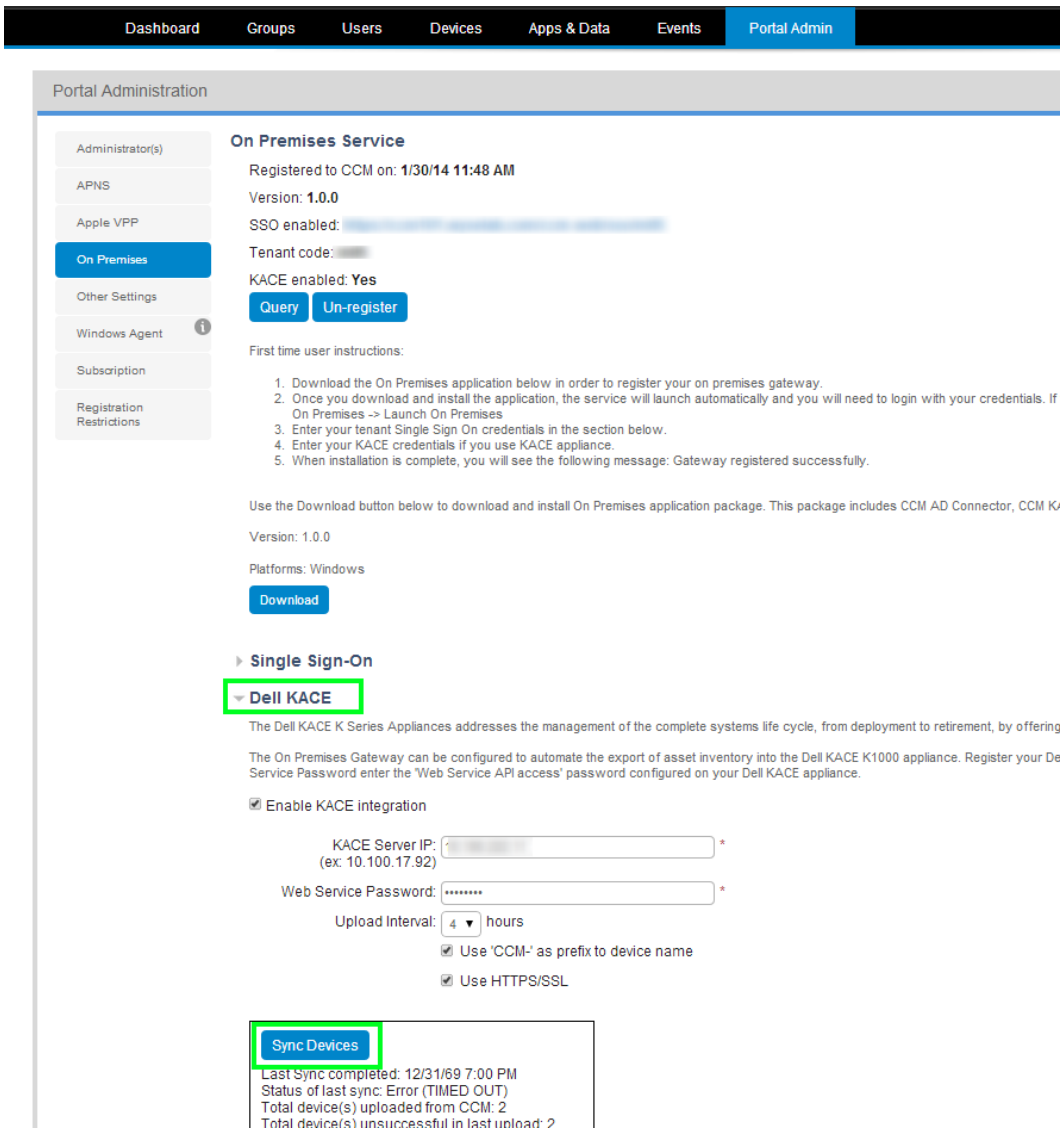




c. **Display Tenant Code and SSO login link**: For Single Sign-On (SSO), the "**Tenant Code**" is now displayed on the On Premises Service page for reference. Additionally, the link used to login to the CCM Administrator portal and self-service page using domain credentials is now displayed at the top of this page next to the label "**SSO enabled**".



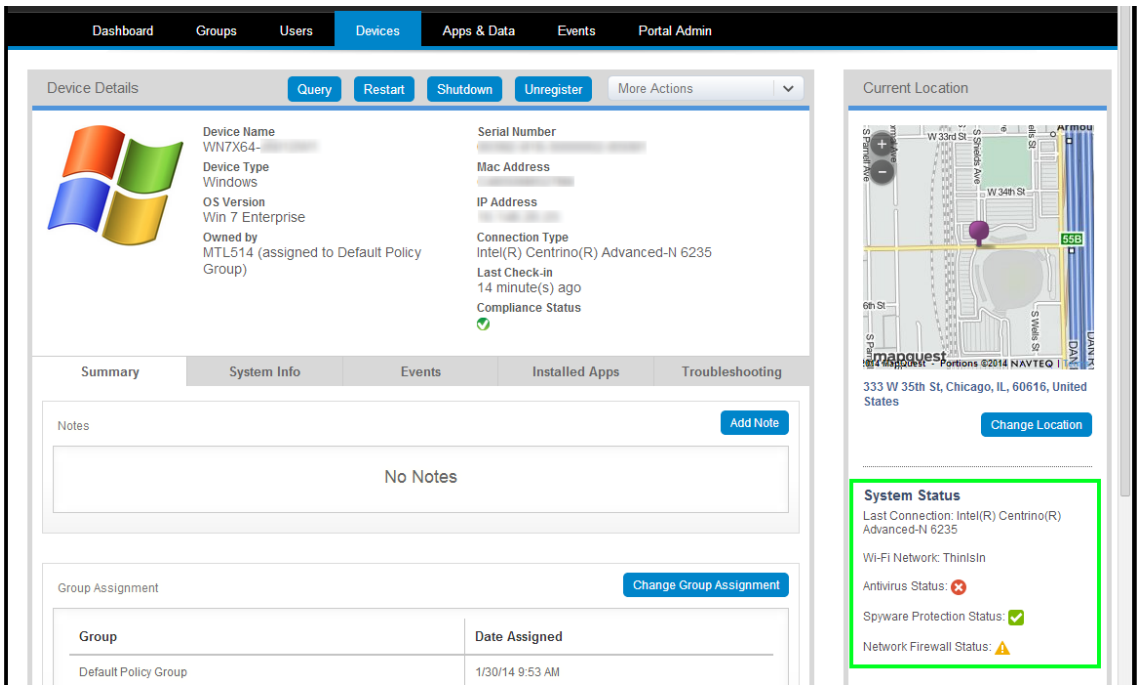
d. **Manually Sync Dell KACE K1000 asset inventory**: When Dell KACE Integration is enabled, use the "**Sync Devices**" button to manually trigger the update of mobile device asset inventory in the Dell KACE K1000 appliance.


Dashboard
Groups
Users
Devices
Apps & Data
Events
Portal Admin
Portal Administration
Administrator(s)
APNS
Apple VPP
On Premises
Other Settings
Windows Agent
Subscription
Registration Restrictions
On Premises Service
Registered to CCM on: 1/30/14 11:48 AM
Version: 1.0.0
SSO enabled:
Tenant code:
KACE enabled: Yes
Query
Un-register
First time user instructions:
1. Download the On Premises application below in order to register your on premises gateway.
2. Once you download and install the application, the service will launch automatically and you will need to login with your credentials. If On Premises -> Launch On Premises
3. Enter your tenant Single Sign On credentials in the section below.
4. Enter your KACE credentials if you use KACE appliance.
5. When installation is complete, you will see the following message: Gateway registered successfully.
Use the Download button below to download and install On Premises application package. This package includes CCM AD Connector, CCM K
Version: 1.0.0
Platforms: Windows
Download
Single Sign-On
Dell KACE
The Dell KACE K Series Appliances addresses the management of the complete systems life cycle, from deployment to retirement, by offering
The On Premises Gateway can be configured to automate the export of asset inventory into the Dell KACE K1000 appliance. Register your De
Service Password enter the 'Web Service API access' password configured on your Dell KACE appliance.
Enable KACE integration
KACE Server IP:
(ex: 10.100.17.92)
Web Service Password:
Upload Interval:
4
hours
Use 'CCM-' as prefix to device name
Use HTTPS/SSL
Sync Devices
Last Sync completed: 12/31/69 7:00 PM
Status of last sync: Error (TIMED OUT)
Total device(s) uploaded from CCM: 2
Total device(s) unsuccessful in last upload: 2

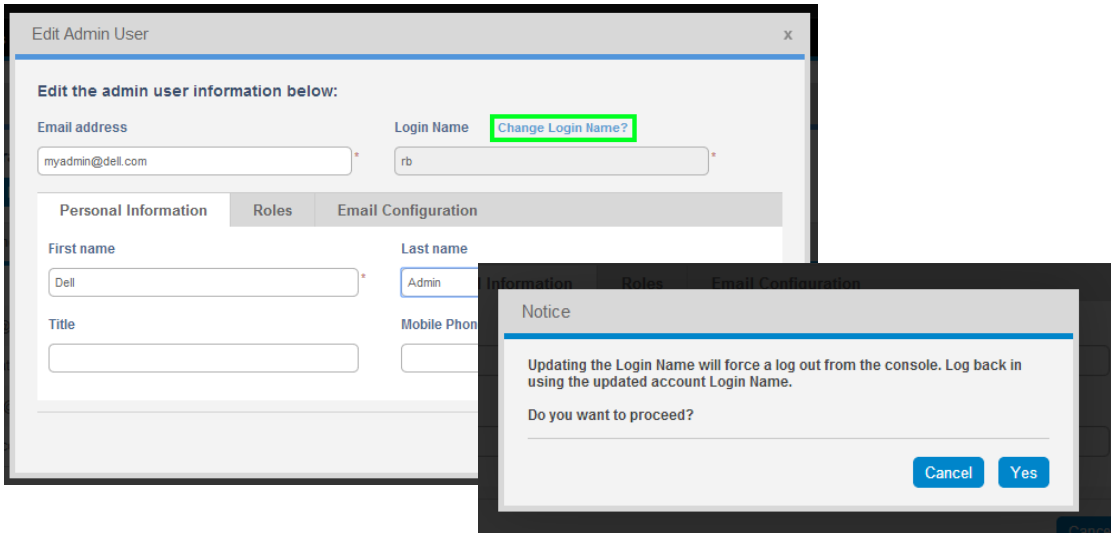
h. **Other Platform Enhancements**

a. **iOS MDM APNS Certificate Enhancements**: Improved messaging during iOS device registration when the iOS MDM APNS certificate is expired or if one is not uploaded to **Portal Admin > APNS**. On the iOS CCM Agent the user will receive warning message for either case. On the Self-Service portal page, if user tries to register from an iOS device and certificate is either not uploaded or expired, the registration button will be disabled with corresponding message underneath.

b. **Updated System Status for Windows Devices**: In the **Device Details** page of Windows Devices, the **System Status** section now displays the last known connection and security settings status for quick visibility.



c. **CCM Administrators updating own login name**: The logged in administrator may change their login name from **Portal Admin > Administrators** by editing account – click "**Change Login Name?**" link to enable this functionality. **NOTE**: This will require a re-login to console.



d. **Dell Mobile Workspace support**. For further information on Dell Mobile Workspace visit: http://software.dell.com/products/container-management-for-mobile-devices/

- ## Supported Devices

Thin Client Requirements

- **Supported Devices:** Thin Clients supported include:
  - C00X (Wyse Xenith) running firmware 2.0_021 or later (**recommended 2.0_105 or later)**
  - R00LX (Wyse Xenith Pro) running firmware 2.0_021 or later (**recommended 2.0_105 or later)**
  - T00X (Xenith 2) running firmware 2.0_021 or later **(recommended 2.0_105 or later)**
  - D00X (Xenith Pro 2) running firmware 2.0_104 or later **(recommended 2.0_105 or later)**
  - C10LE running firmware ThinOS 7.1_207 or later(**recommended 8.0_210 or later)**
  - R10L running firmware ThinOS 7.1_207 or later (**recommended 8.0_210 or later)**
  - T10 running firmware ThinOS 7.1_207 or later (**recommended 8.0_210 or later)**
  - T10D running firmware ThinOS 8.0_210 (new platform added)
  - D10D running firmware ThinOS 8.0_037 or later (**recommended 8.0_211 or later)**
  - D10DP running firmware ThinOS 8.0_117 or later (**recommended 8.0_211 or later)**
  - Z10DP running firmware ThinOS 8.0_037 or later (**recommended 8.0_211 or later)**

  ***Refer to CCM support site for updates on supported devices:
  https://support.cloudclientmanager.com/entries/22579541

  For supported thin clients running earlier versions, a firmware update is required to enable Cloud Client Manager connectivity. Updates can be downloaded from the Wyse Self-Service Center at: http://support.wyse.com/selfservice.html

  IMPORTANT: You must use your *ThinOS Maintenance* (you should have received an email from Wyse or your reseller with full instructions) to obtain available firmware updates (if you did not receive this email, contact your reseller). If unfamiliar with updating firmware on Wyse ThinOS cloud clients, refer to Wyse Knowledge Base Solution #**10566** (go to Wyse Knowledge Base at http://www.wyse.com/kb and search for **10566**).

- **Connectivity Requirements:**
  - TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com

iOS Requirements

- **Supported Devices:**
  - iPhone, iPad, iPod Touch devices running iOS Version 5.x and later

- **Connectivity Requirements:**
  - TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 80 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 8443 (outbound) to us1-mdm.cloudclientmanager.com
  - TCP port 5223 (outbound) - for Apple APNS

- **MDM Certificate Requirements:**
  - A Mobile Device Management (MDM) Apple Push Notification Service (APNs) certificate is required for iOS device management - this requires an Apple ID. As the Apple ID account will be linked to the APNs certificate, which must be renewed annually, a corporate Apple ID account should be used and not a personal one

Android Requirements

- **Supported Devices:**
  i. Devices running Android Version 2.3 and later

- **Connectivity Requirements:**
  i. TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  ii. TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com

Dell Wyse Cloud Connect Requirements

IMPORTANT: Dell Wyse Cloud Connect devices require a valid Cloud Client Manager user account in order to register device during the device activation process.

- **Supported Devices:**
  i. Android Version 4.1 and later

- **Connectivity Requirements:**
  i. TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  ii. TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com

On Premises Gateway Requirements

- **Supported Devices:**
  i. Windows machine running Windows 7, Windows 8
  ii. Minimum CPU requirements: 1 GHz (x86 processor) or 1.4 GHz (x64 processor)
  iii. Minimum available RAM: 1 GB
  iv. Minimum Disk Space: 2 GB available (for install and maintaining service operation)

- **Connectivity Requirements:**
  i. TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  ii. TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com

  NOTE: The On Premises Gateway must be installed on a server within the DMZ externally accessible, and the fully qualified domain name (FQDN) of the server must be registered in public DNS.

Windows Agent Requirements

- **Connectivity Requirements:**
  - TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com
- **OS Requirements:**

Windows Version	OS Architecture	
	32-bits	64 - bits
Windows 8 / Pro / Enterprise	YES	YES
Windows 7 Starter / Home Basic / Home Premium / Professional / Enterprise / Ultimate – Service Pack 1	YES	YES
Windows Server 2012 Standard / Essential / Datacenter / Foundation – Service Pack 1	YES	YES
Windows Web Server 2008 R2 – Service Pack 1	**N/A**	YES
Windows Storage Server 2008 R2 – Service Pack 1	**N/A**	YES
Windows Server 2008 R2 Standard Ed. / Enterprise Ed. / Datacenter Ed. – Service Pack 1	**N/A**	YES
Windows Server 2008 R2 for Itanium-based Systems - Service Pack 1	**N/A**	YES
Windows HPC Server 2008 R2 for high Performance supercomputers - Service Pack 1	**N/A**	YES
Windows Server 2008 R2 Foundation - Service Pack 1	**N/A**	YES
Windows Web Server 2008	YES	YES
Windows Server 2008 Standard Edition (Microsoft Windows NT 6.0 6002 Service Pack 2)	YES	YES
Windows Server 2008 Enterprise Edition (Microsoft Windows NT 6.0 6001 Service Pack 1)	YES	YES
Windows Server 2008 Datacenter Edition	YES	YES
Windows Storage Server 2008	YES	YES
Windows Small Business Server 2008	YES	YES
Windows Essential Business Server 2008	YES	YES
Windows Server 2008 for Itanium-based Systems	YES	YES
Windows HPC Server 2008 for high Performance supercomputers	YES	YES
Windows Server Foundation 2008	YES	YES

Known Issues

STR-678	iOS registration fails if re-registering within 30 seconds
STR-842	Some iOS/Android sub-options at lower policy level not affected by changes to parent options at higher policy level
STR-1148	Android device prompts for app install for installed System apps
STR-1173	Remove certificate for iOS payload fails unless linked payload is removed
STR-1409	Picture taken from the Android back camera compressed on Agent display (correct on server)
STR-1497	iOS Webclip uploaded image truncated in IE8 in CCM console
STR-2335	User/Device Details summary view not displaying some iOS settings when payload configured at higher level is saved with default settings at user/device level.
STR-2414	Event missing when removing device-level exception payloads
STR-2449	Cannot deactivate AD user missing email address
STR-2489	Apps installed from App Store not tagged as “not managed” in CCM Agent when user cancels the app install request on device
STR-2729	During Thin Client registration, in specific scenario device shows as compliant even if configuration could not be loaded.
STR-3009	In Thin Client system information, the “802.1X Auth” field may report N/A when invalid characters received
STR-3137	User prompted to reinstall enterprise app when changing group and app assigned to both groups (iOS)
STR-4187	Advanced RDP settings may be sent if checkbox is unchecked
STR-4370	App policies are not unassigned for AD synced groups when they are no longer synced
STR-4374	SSO login fails if email address is changed in AD
STR-4615	Reloading the same certificate on On Premises Gateway fails
STR-4621	When unregistering On Premises Gateway the page needs to be refreshed to see status update

Issues resolved in this release

CPC-365	Pagination added to top of Installed App tab on Device Details page
STR-3096	Thin client details displaying device name instead of SSID for Current Wi-Fi Network.
STR-3200	iOS CCM Agent updates managed app states on check-in
STR-4090	Republish for iOS AirPrint, AirPlay, Fonts payloads
STR-4198	Prevent On Premises Gateway registration if one already registered
STR-4230	Other filters do not display any results after selecting AppSDK filter in Users page
STR-4285	Remove unsupported iOS option – Header Magic in Exchange ActiveSync payload
STR-4306	Export Devices to CSV feature not working in IE8
STR-4323	iOS CCM Agent not updating status for deactivated mobile user
STR-4347	iPod Touch minimum OS version not enforced correctly

Release Notes for Previous Releases

"R4" Release (December 8, 2013)

- **Release Overview**

The Cloud Client Manager "R4" release includes a lot of new functionality for both the platform and for device management on all device types. Amongst these changes are an updated look & feel, the new On-Premises Gateway, and enhanced support for Thin Client, iOS, Android and Dell Wyse Cloud Connect management.

Some of the highlights include:

- **Enhanced Look & Feel**
  - Updated Cloud Client Manager console look and feel
  - Updated Cloud Client Manager Agent for Android and Dell Cloud Connect devices with better feedback and usability enhancements

- **New On-Premises Gateway *[PRO tier only]***
  - New application installed on-premises provides extended functionality to the Cloud Client Manager features offered in the cloud:
    - **Single Sign-On support**: Portal administrators and mobile users can now use domain credentials for portal authentication (Administrator and Self-Service views) and for mobile device registration.
    - **Dell KACE K1000 Integration**: Ability to automate export of asset inventory into Dell KACE K1000 appliance.
    - **AD Connector bundled installation**: Use for bulk import and manual sync of AD Groups and Users with the Cloud Client Manager portal, the AD Connector is now bundled with the On-Premises Gateway installer.

- **Enhanced Thin Client features**
  - Expanded set of settings for configuring ThinOS and Xenith devices; this requires latest thin client firmware. See Cloud Client Manager support site for details.
  - Tech Preview of support for Windows Embedded (WES7 and WE8S) thin clients
  - Support for 10 additional custom INI parameter values for thin clients

- **Enhanced iOS device support**
  - New Apple VPP program (for iOS 7 devices) ***[PRO tier only]***
  - New iOS 7 device payloads (AirPrint, AirPlay, Fonts)
  - New iOS 7 device options for device restrictions (lock screen views, fingerprint unlock) and Wi-Fi policies
  - Support for Dell SonicWALL Mobile Connect and Cisco AnyConnect VPN clients

- **Enhanced Android device support**
  - Enterprise Wi-Fi management (with certificates)
  - VPN support for Dell SonicWALL Mobile Connect and Cisco AnyConnect

- **New Registration Restrictions policies**
  - Block mobile device registration by number of devices registered per user (total and by device type) and by minimum OS version

- **Platform Enhancements**:
  - Enhancements for Apple APNS certificate management
  - Enhancements to Users page
  - Enhancements to email message templates for user invitations
  - Added support for modifying login name for Portal Administrators

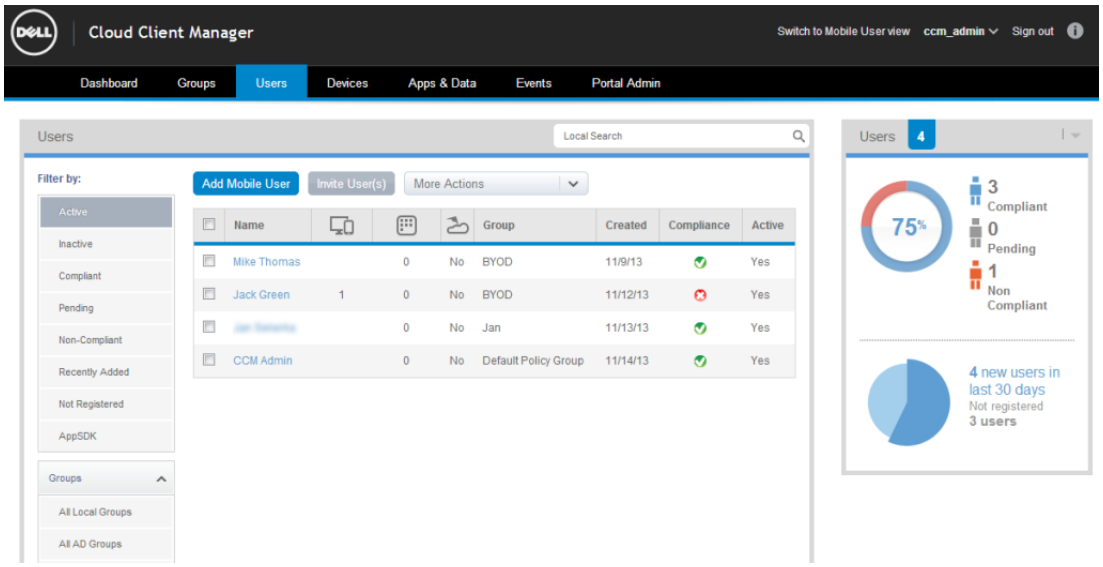
- **New Device Encryption policy**
  - Compliance and visibility into device encryption for iOS and Android devices

- **Introduction of "Keystone" (Currently in Private Beta) *[PRO tier only]***:
    - A new workspace for iOS and Android devices enabling secure container on device for access to corporate content and resources. The following secure apps are supported: email, calendar, contacts, file browser, web browser.

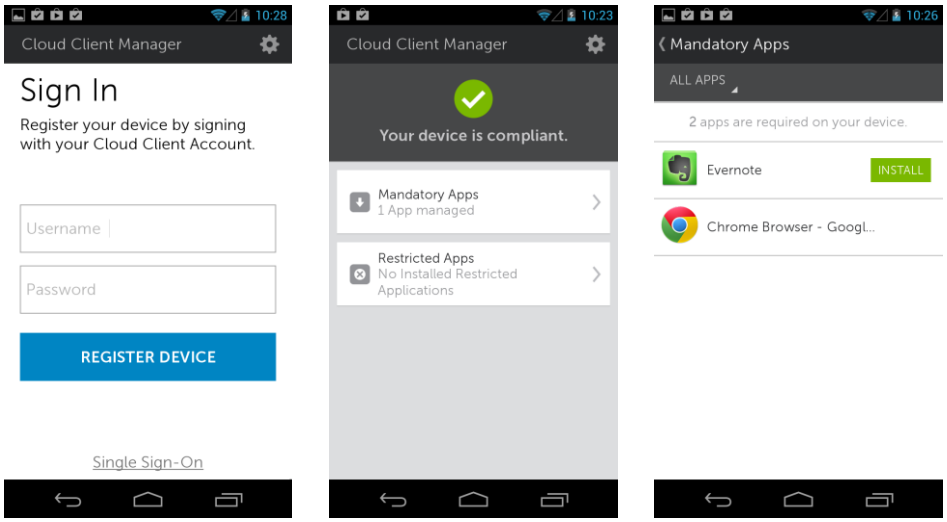
- **New Features Details**

1. **<u>New Cloud Client Manager console look & feel and update to Android Agent User Interface</u>**

   - Update to the Cloud Client Manager console colors and views:



   - New look & feel for Android CCM Agent for enhanced user experience and guidance on how to remediate Non-Compliant devices.



2. New Cloud Client Manager On-Premises Gateway *[Available for PRO tier only]*

The Cloud Client Manager On-Premises Gateway is an application that can be installed on-premises as an extension to the Cloud Client Manger functionality provided in the cloud.

By installing and configuring this gateway the following features can be enabled:

a. **Single Sign-On**: Support for Single Sign-On for portal authentication (Admin and Self-Service views) and for mobile device registration. Portal administrators and mobile users can now use domain credentials instead of local Cloud Client Manager credentials for these functions.

b. **Dell Kace K1000 Integration**: Ability to automate export of asset inventory into the Dell Kace K1000 appliance.

c. **AD Connector**: The AD Connector is now bundled with the On-Premises Gateway installer. This allows for bulk import and manual sync for AD Groups and Users with the Cloud Client Manager portal.

The On-Premises gateway can be downloaded from **Portal Admin > On Premises**.

For more details on the On-Premise gateway refer to the "**On-Premises Gateway Overview**" support article: https://support.cloudclientmanager.com/entries/30600507

3. Enhanced Thin Client management features:

The following enhancements are available in this release for Thin Client management:

a. Thin Client Support

I. Support for WES7 and WE8S thin clients [**Tech Preview**]

Focus of this Tech Preview is on monitoring and visibility of the Windows Embedded thin client assets.

i. Use the Windows agent (from **Portal Admin > Windows Agent**) and install it on a thin client after disabling Write-Filter, enter tenant group key, and then enable the Write-Filter).

ii. Registration

iii. Inventory

- Hardware
- Software
- Network
- Security status
  - Anti-virus
  - Anti-spyware
  - Firewall
  - Windows Update
  - Internet security

iv. Grouping (no additional functionality is supported other than assigning devices to Groups)

v. Real-time Commands

- Restart
- Shutdown

- Send a message to user
- Query for updated device information

vi. Troubleshooting

- Screenshot (with/without user permission)
- Process list (option to End a process)
- Services list (option to Restart/Shutdown a service)
- Performance monitoring

II. Support for new/updated Wyse ThinOS and Xenith devices

i. D10DP – new platform that adds PCoIP support for connecting to VMware Horizon View in addition to Citrix, RDP and RDS/Terminal Server environments

ii. T10D – new dual-core ARM platform (releasing soon)

b. <u>New Settings</u>

I. Visual Experience

i. Prevent toolbar from closing unless mouse focus moves away

ii. Auto-hide toolbar after specified seconds

iii. Desktop Wallpaper

- Wallpaper image can be uploaded from the 'Apps & Data' tab

II. Security

i. Allow lockdown of device (Save Privilege level in local flash)

ii. Require domain login to use device

iii. Disable guest users

iv. Require reentering password after Sign-on

v. Require smartcard for login

vi. Require smartcard for login

vii. Disable WDM Service

viii. Disable ThinPrint Service

ix. Disable VNC Shadowing

x. Fast Disconnect Key (Use F12 to disconnect Citrix sessions)

III. Remote Connections

i. Broker server for Quest vWorkspace

ii. Detailed Session Behavior Defaults for all connection types

iii. Peripheral Behavior

- Auto-connection to selected local device types
- USB redirection

iv. Direct RDP connection settings

v. Microsoft RDS/Terminal Server settings

vi. Citrix

- Use default settings for XenApp and XenDesktop or provide customized settings for HDX
- Additional settings including as session reconnection, self-service center, authentication method, Reset VM, 32-bit icons.

vii. VMware

- Protocol: RDP/PCoIP

IV. Other
    i. Remember previous username
    ii. TimeZone
        - Daylight Savings Time (DST)

V. Advanced
    i. Set up to 20 INI parameters (increased from 10)

c. Removed Settings

I. Remote Connections: Enable Branch Repeater for Citrix (this has been deprecated by Wyse ThinOS)

Refer to following support article for updates on Thin Client features:
https://support.cloudclientmanager.com/entries/30062368

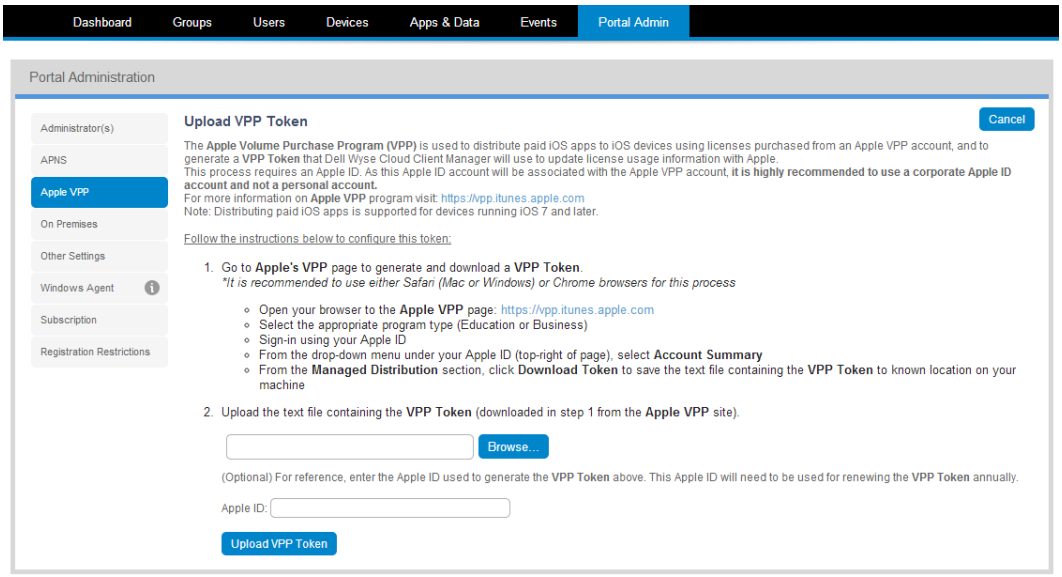
4. Enhanced iOS device support

a. Support for new Apple VPP program (iOS 7 devices) *[Available for PRO tier only]*

From **Portal Admin > Apple VPP**, can configure your Apple VPP account to distribute licenses to users for paid iOS apps (only iOS 7+ devices are supported).

By uploading the VPP Token provided by Apple via the VPP Account, Cloud Client Manager is able to sync with your account for user status and license usage.

For more details on configuring the Apple VPP feature, consult the **Apple VPP for iOS 7 Overview** support article: https://support.cloudclientmanager.com/entries/30832357


Dashboard
Groups
Users
Devices
Apps & Data
Events
Portal Admin
Portal Administration
Administrator(s)
APNS
Apple VPP
On Premises
Other Settings
Windows Agent
Subscription
Registration Restrictions
Upload VPP Token
Cancel
The Apple Volume Purchase Program (VPP) is used to distribute paid iOS apps to iOS devices using licenses purchased from an Apple VPP account, and to generate a VPP Token that Dell Wyse Cloud Client Manager will use to update license usage information with Apple.
This process requires an Apple ID. As this Apple ID account will be associated with the Apple VPP account, it is highly recommended to use a corporate Apple ID account and not a personal account.
For more information on Apple VPP program visit: https://vpp.itunes.apple.com
Note: Distributing paid iOS apps is supported for devices running iOS 7 and later.
Follow the instructions below to configure this token:
1. Go to Apple's VPP page to generate and download a VPP Token.
*It is recommended to use either Safari (Mac or Windows) or Chrome browsers for this process
Open your browser to the Apple VPP page: https://vpp.itunes.apple.com
Select the appropriate program type (Education or Business)
Sign-in using your Apple ID
From the drop-down menu under your Apple ID (top-right of page), select Account Summary
From the Managed Distribution section, click Download Token to save the text file containing the VPP Token to known location on your machine
2. Upload the text file containing the VPP Token (downloaded in step 1 from the Apple VPP site).
Browse...
(Optional) For reference, enter the Apple ID used to generate the VPP Token above. This Apple ID will need to be used for renewing the VPP Token annually.
Apple ID:
Upload VPP Token

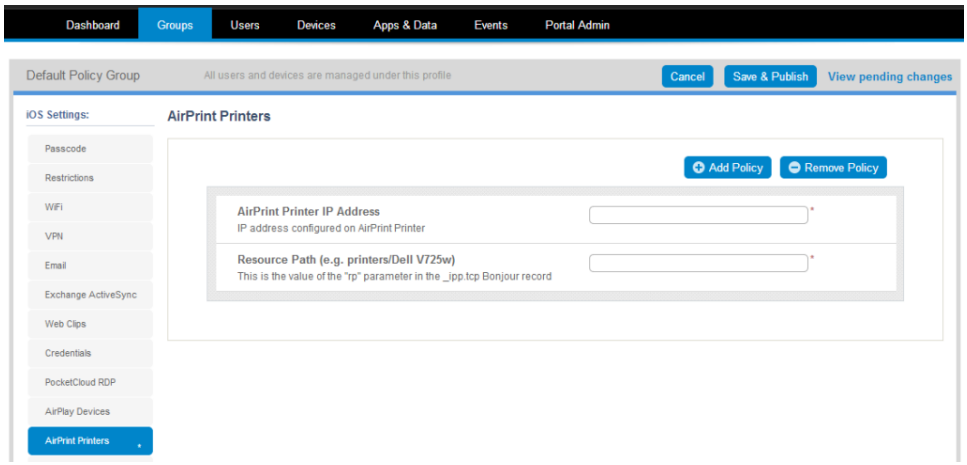
NOTE: Apple VPP for pre-iOS 7 devices is not supported with this release.

b. New iOS 7 payloads (AirPrint, AirPlay, Fonts)

Support for the following payloads has been added in this release: AirPrint Printers, AirPlay Devices, Fonts. These payloads are only supported on iOS devices running iOS 7+.

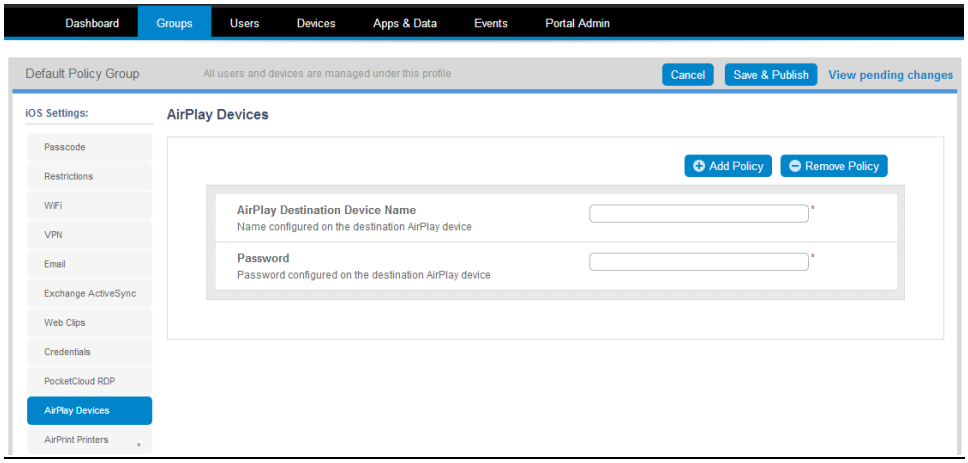
I. AirPrint Printers

Available from **iOS Settings > AirPrint Printers**, this allows AirPrint printers to be pre-configured for iOS 7+ devices. To configure the printer the IP Address and Resource Path of the printer must be known. The Resource Path corresponds to the "**rp**" parameter of the printers **_ipp.tcp** Bonjour record (e.g. *printers/Dell V725w*).



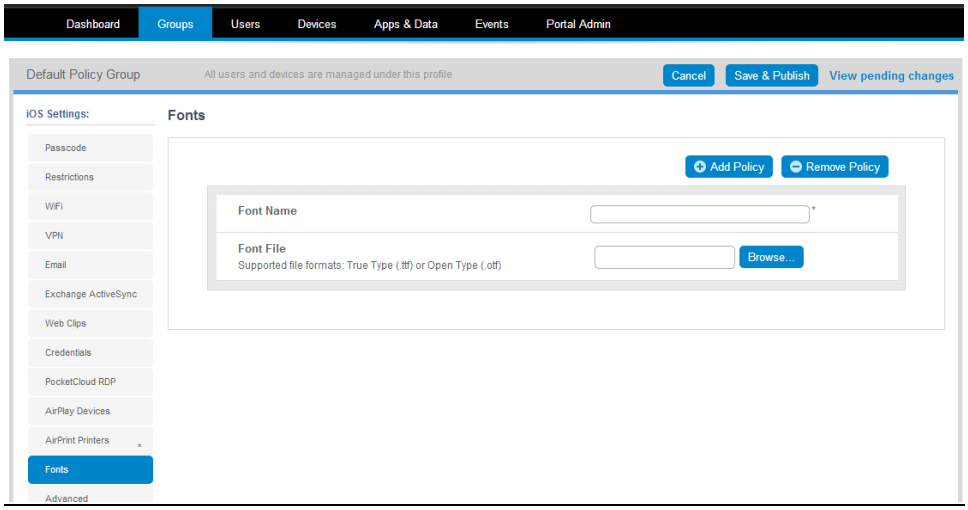
II. AirPlay Devices

Available from **iOS Settings > AirPlay Devices**, this allows AirPlay devices to be pre-configured for iOS 7+ devices. To add an AirPlay device, the device name and password must be configured.



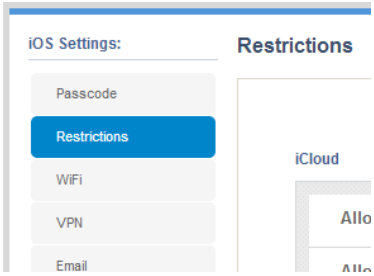
III. Fonts

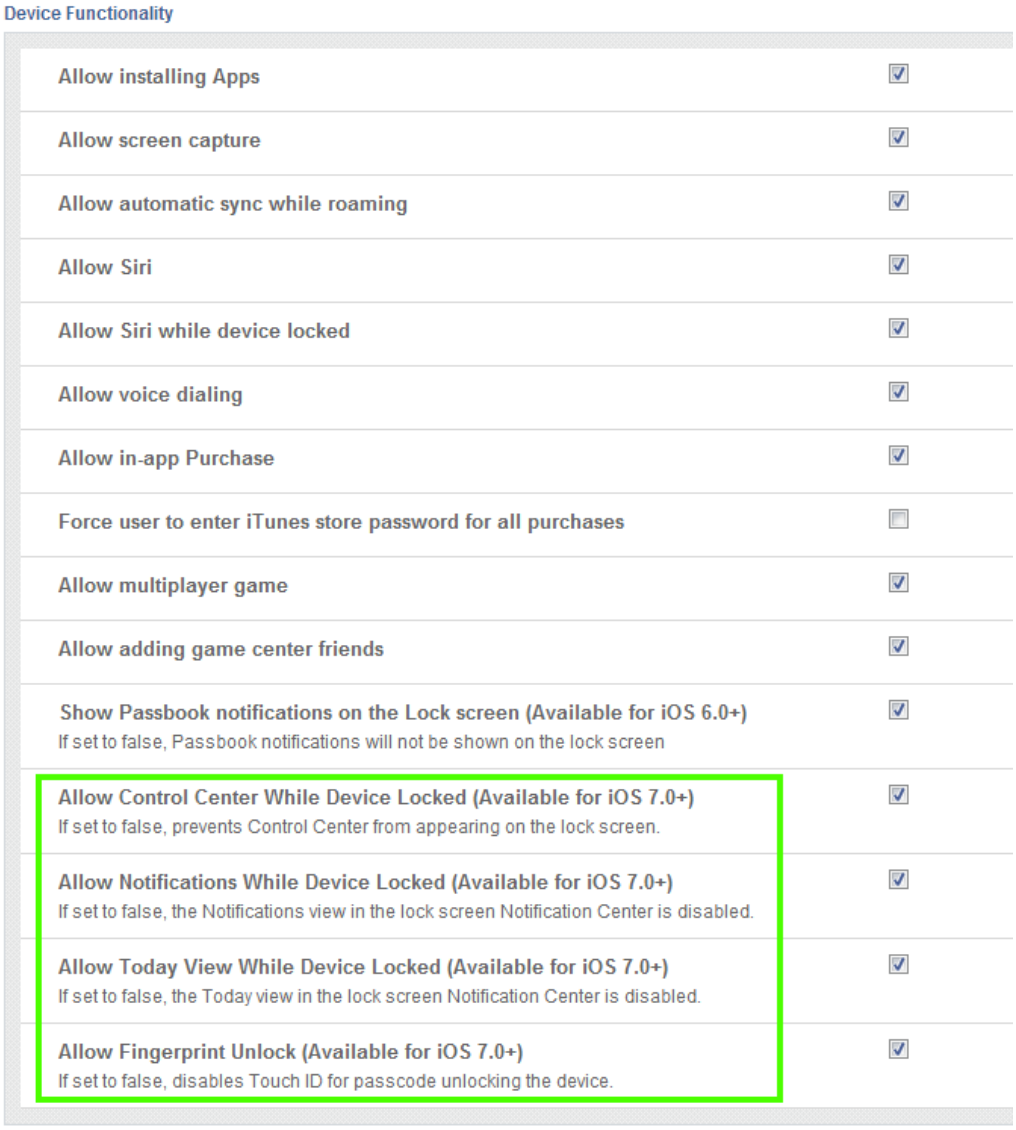
Available from **iOS Settings > Fonts**, this allows True Type (.ttf) or Open Type (.otf) font files to be send to iOS 7+ devices. The font will be identified on the device by the Postscript name embedded in the fonts file.



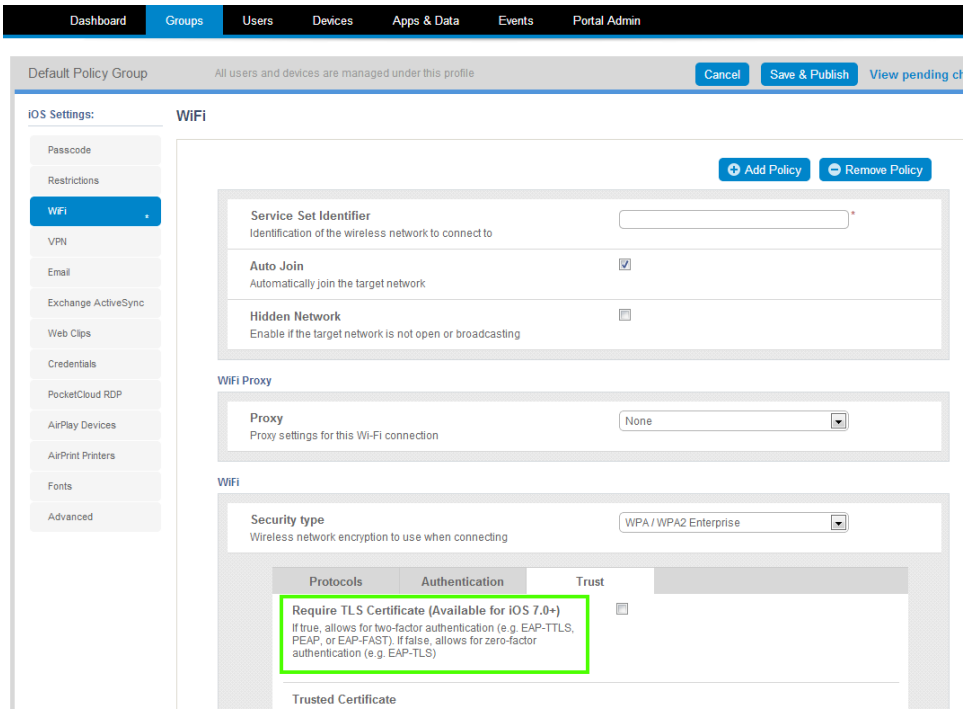
c. New iOS 7 options for device restrictions (lock screen views, fingerprint unlock) and Wi-Fi policies

- Available from **iOS Settings > Restrictions**, the following device restrictions are now available for iOS 7+ devices:
  - **Allow Control Center While Device Locked**: Option to manage Control Center on the lock screen
  - **Allow Notifications While Device Locked**: Option to manage the Notifications view in the lock screen Notification Center
  - **Allow Today View While Device Locked**: Option to manage the Today view in the lock screen Notification Center
  - **Allow Fingerprint Unlock**: Option to manage the Touch ID for device passcode unlocking




Device Functionality
Allow installing Apps
Allow screen capture
Allow automatic sync while roaming
Allow Siri
Allow Siri while device locked
Allow voice dialing
Allow in-app Purchase
Force user to enter iTunes store password for all purchases
Allow multiplayer game
Allow adding game center friends
Show Passbook notifications on the Lock screen (Available for iOS 6.0+)
If set to false, Passbook notifications will not be shown on the lock screen
Allow Control Center While Device Locked (Available for iOS 7.0+)
If set to false, prevents Control Center from appearing on the lock screen.
Allow Notifications While Device Locked (Available for iOS 7.0+)
If set to false, the Notifications view in the lock screen Notification Center is disabled.
Allow Today View While Device Locked (Available for iOS 7.0+)
If set to false, the Today view in the lock screen Notification Center is disabled.
Allow Fingerprint Unlock (Available for iOS 7.0+)
If set to false, disables Touch ID for passcode unlocking the device.

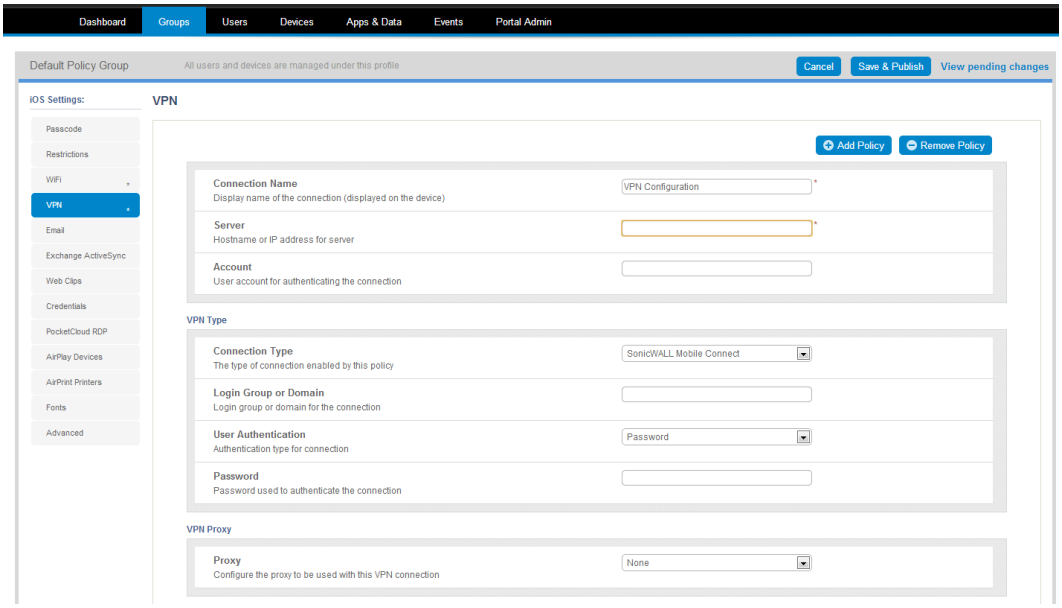
- Available from **iOS Settings > WiFi**, new option “Require TLS Certificate” for iOS 7+ devices. Allows for management of trusted certificates for WPA/WPA2-Enterprise Wi-Fi networks.



d. VPN support for Dell SonicWALL Mobile Connect and Cisco AnyConnect

Available from **iOS Settings > VPN**, this allows for VPN profiles to be distributed to iOS devices. With this release the following VPN clients are supported:

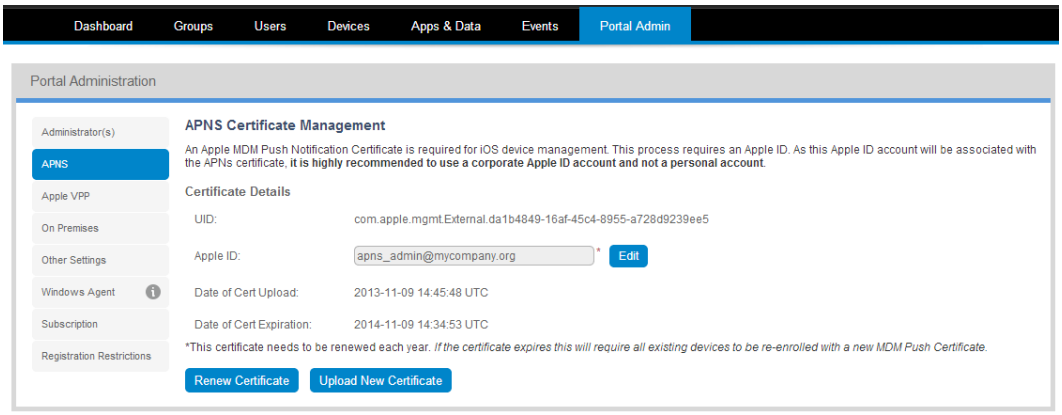
- Dell SonicWALL Mobile Connect
- Cisco AnyConnect



e. Enhanced Apple APNS certificate management

Updates to the **Portal Admin > APNS** page to simplify renewal of APNS certificates for MDM device management:

- New "**Renew Certificate**" button providing specific instructions for renewal of Apple APNS certificate
- Option to store the **Apple ID** used to create the certificate (NOTE: this **Apple ID** will need to be used annually to renew the certificate)
- New portal notification that will appear on the **Dashboard** if the certificate will expire within 30 days


Dashboard
Groups
Users
Devices
Apps & Data
Events
Portal Admin
Portal Administration
Administrator(s)
APNS
Apple VPP
On Premises
Other Settings
Windows Agent
Subscription
Registration Restrictions
APNS Certificate Management
An Apple MDM Push Notification Certificate is required for iOS device management. This process requires an Apple ID. As this Apple ID account will be associated with the APNs certificate, it is highly recommended to use a corporate Apple ID account and not a personal account.
Certificate Details
UID:
com.apple.mgmt.External.da1b4849-16af-45c4-8955-a728d9239ee5
Apple ID:
apns_admin@mycompany.org
Edit
Date of Cert Upload:
2013-11-09 14:45:48 UTC
Date of Cert Expiration:
2014-11-09 14:34:53 UTC
*This certificate needs to be renewed each year. If the certificate expires this will require all existing devices to be re-enrolled with a new MDM Push Certificate.
Renew Certificate
Upload New Certificate

5. Enhanced Android Device Support

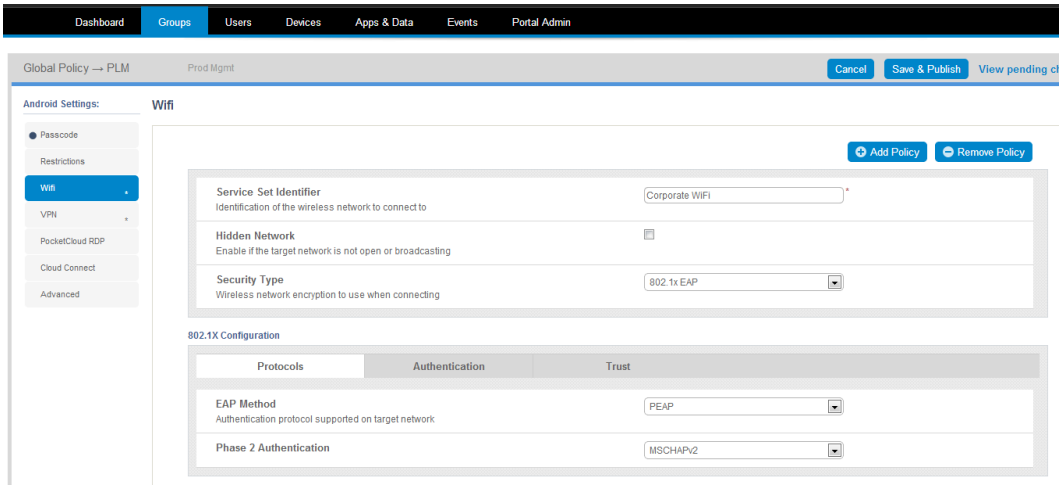
a. Enterprise Wi-Fi management (with certificates)

Available from **Android Settings > WiFi**, enhancements to distribute enterprise "802.1X EAP" enterprise Wi-Fi profiles:

- Streamlined configuration for EAP Method types
- Ability to distribute certificates for Trusted CA Certificates and for EAP-TLS identity certificates.

  NOTE: Certificate installation is supported for devices running minimum Android version 4.0 ("Ice Cream Sandwich"). For pre-"Jelly Bean" (Android 4.1) devices the user may need to manually assign the certificate to the Wi-Fi profile if the device cannot match the name of the certificate.

  NOTE 2: Cloud Client Manager initiates the certificate installation on device (requires user interaction to complete install). Once installed certificates cannot be removed by CCM Agent – if required, certificates must be removed locally.

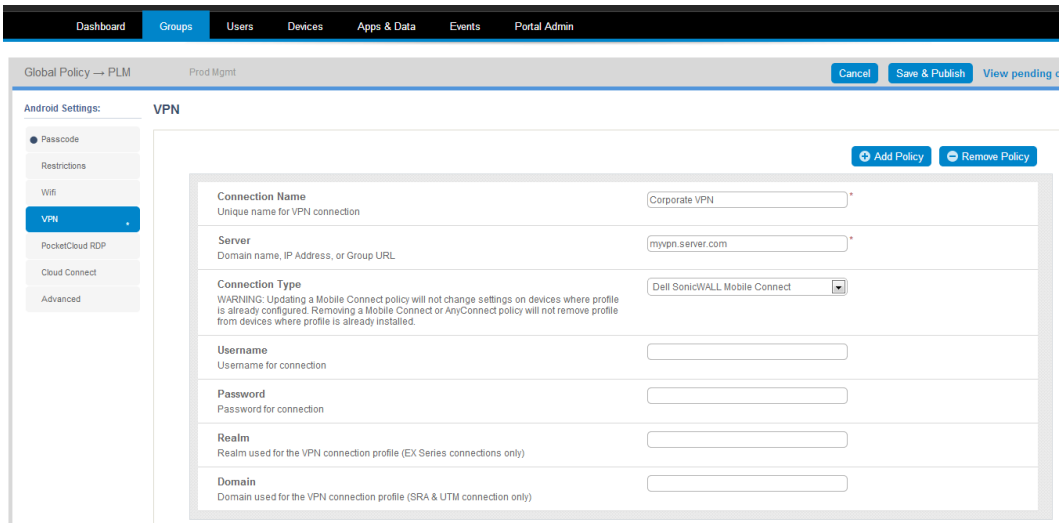


b. VPN support for Dell SonicWALL Mobile Connect and Cisco AnyConnect

Available from **Android Settings > VPN**, this allows for VPN profiles to be distributed to Android devices. With this release the following VPN clients are supported:

- Dell SonicWALL Mobile Connect
- Cisco AnyConnect

NOTE: For **Cloud Client Manager** to create Cisco AnyConnect profiles on the device the option "**Settings > External Connection**" must be set to either "**Enabled**" or "**Prompt**" (user will be requested to accept profile) in the Cisco AnyConnect app on device.



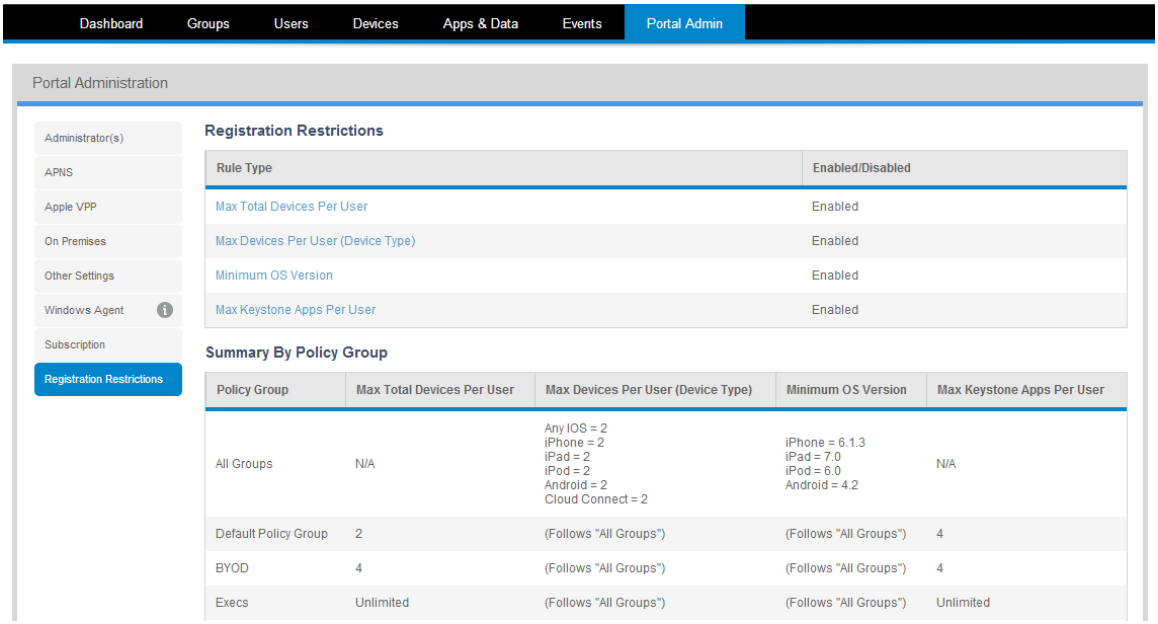
NOTE: Dell SonicWALL Mobile Connect and Cisco AnyConnect profiles can be distributed one time from the CCM console – however, they cannot be removed or updated on the device. To update profiles it is recommended to create a new VPN profile with the updated settings. Changes to existing profiles will only affect devices registered with Cloud Client Manager after the change has been made, if the profile does not already exist on device.

6. New Registration Restrictions for Mobile Devices

This feature allows rules to be configured to block mobile device registration if specific device criteria are not met. The following rules are configurable:

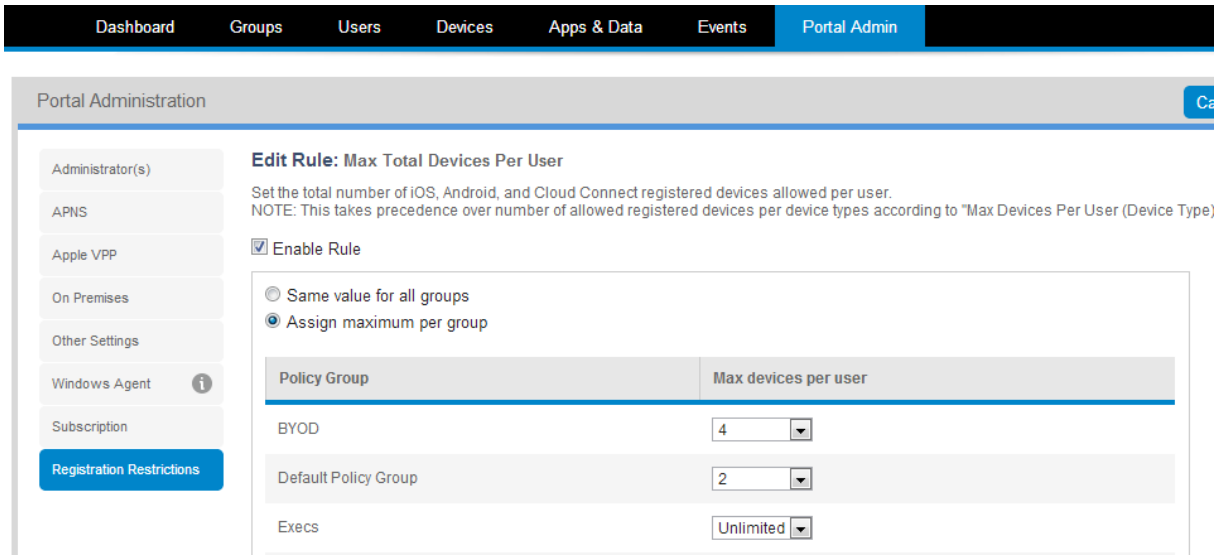
- **Max Total Devices Per User**: The total number of iOS, Android, and Cloud Connect devices registered allowed per user.
- **Max Devices Per User (Device Type)**: The number or iOS, Android and Cloud Connect devices registered allowed per user. For iOS devices a rule can be configured for the total number of iOS devices or by iOS device model (iPhone, iPad, iPod). Both **Total iOS** and specific iOS models may be configured, however total for individual iOS types cannot exceed value set for the **Total iOS** – e.g. if **Total iOS** / **iPhone** / **iPad** / **iPod** are all set to '**2**', any combination of iPhone, iPad, and iPad may be registered as long as total does not exceed two devices registered.

  NOTE: User cannot register more devices than allowed by the **Max Total Devices Per User** rule.
- **Minimum OS Version**: Configure the minimum OS version for device registration. Supported for iOS (iPhone, iPad, iPod) and Android. Version number supports up to 3 decimal places .
- **Max Keystone Apps Per User**: The total number of Keystone apps registered allowed per user.



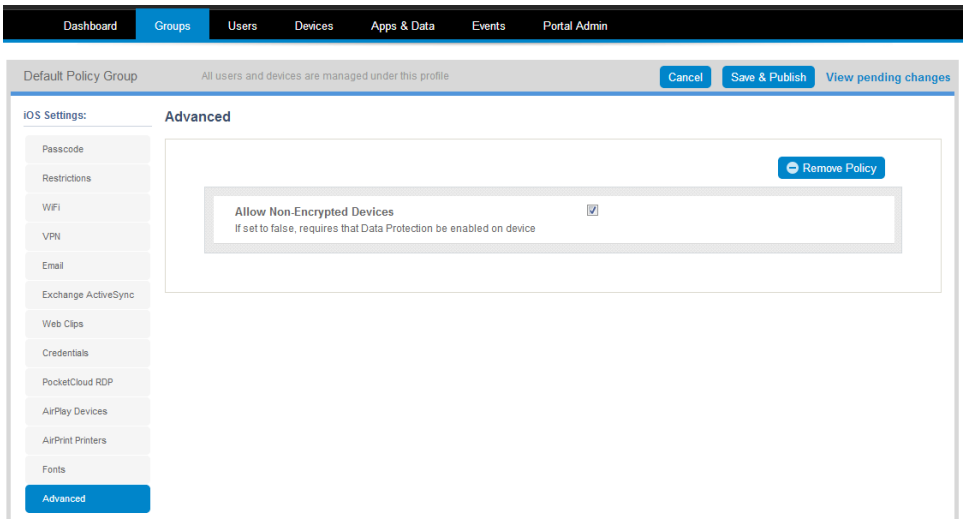
Each registration rule can be configured as same value for all Policy Groups, or can be set individually per group. To configure a rule, click on the rule name and select the "Enable Rule" checkbox.

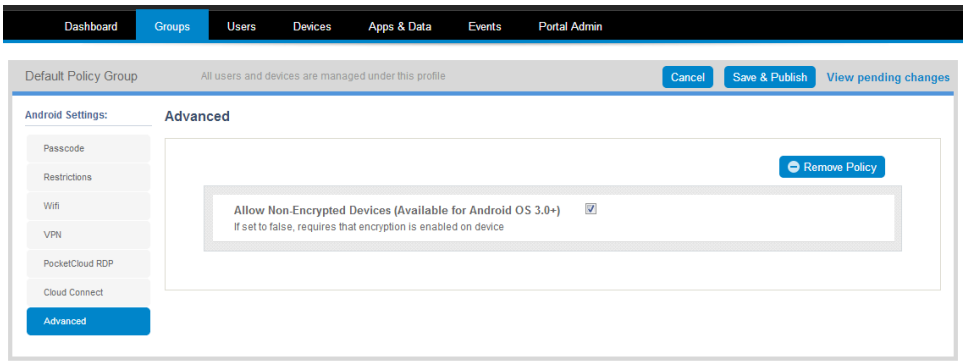
To configure the same policy for all groups select the "**Same value for all groups**" option. Otherwise, select the option to configure on a per-Policy Group basis.



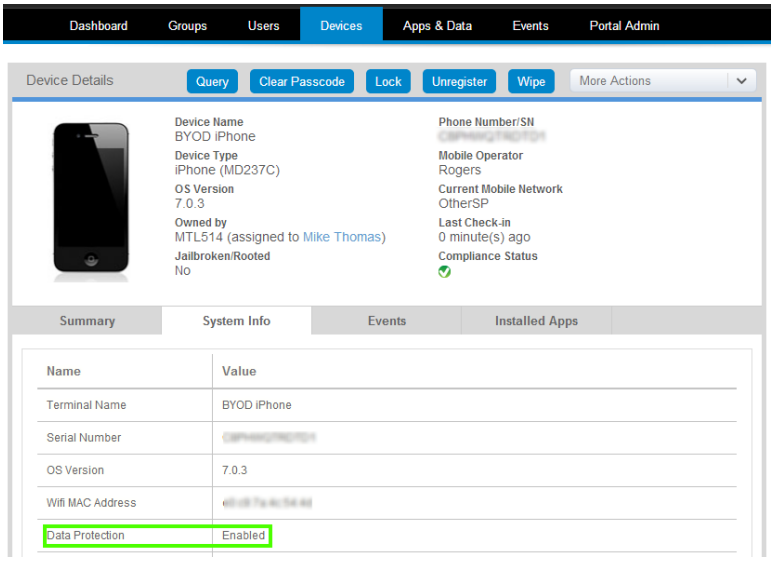
7. Visibility into device encryption for iOS and Android devices

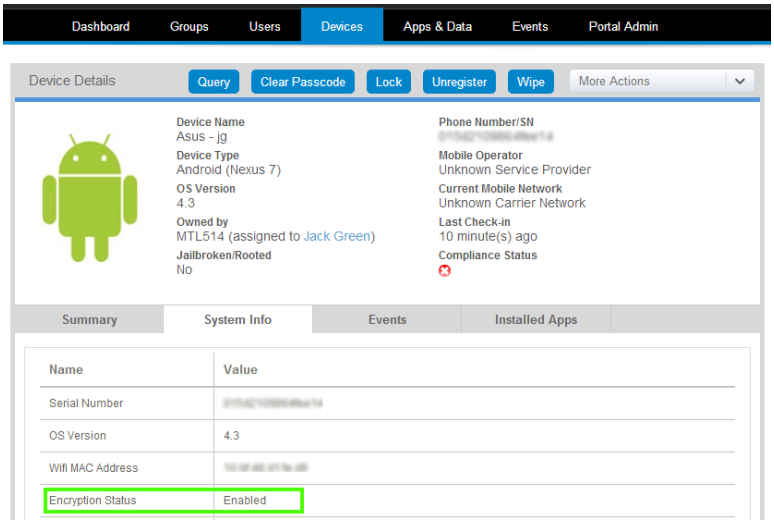
New policy that allows for device encryption to be considered for device compliance. For iOS, this policy provides visibility into of the iOS **Data Protection** is enabled on the device – policy is configured from iOS **Settings > Advanced**. For Android, this is supported for devices running Android OS 3.0+ - the policy is configured from **Android Settings > Advanced**.





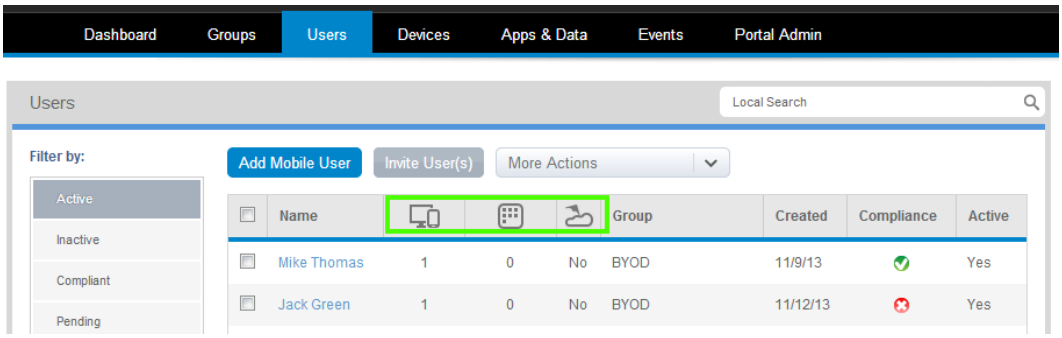
The Data Protection / Encryption status is visible from the **Device Details > System Info** tab. If the device is not compliant with the policy, then an alert will be flagged until the device becomes compliant.





8. Platform Enhancements

a. **Enhancements to Users Page**: In the table there are new icons for the columns to see number of devices and Keystone apps registered to a user, in addition to if user has used Cloud Client Manager credentials to login from PocketCloud app.



Where:

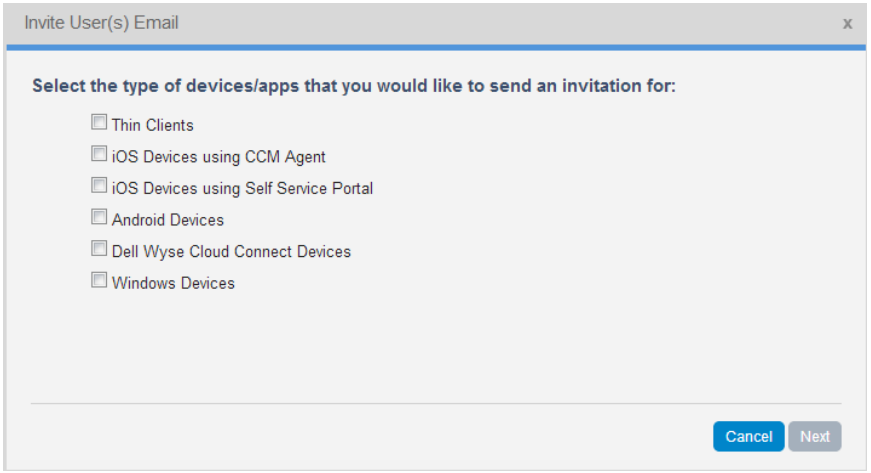
= Number of devices registered by user

= Number of Keystone workspaces registered by user

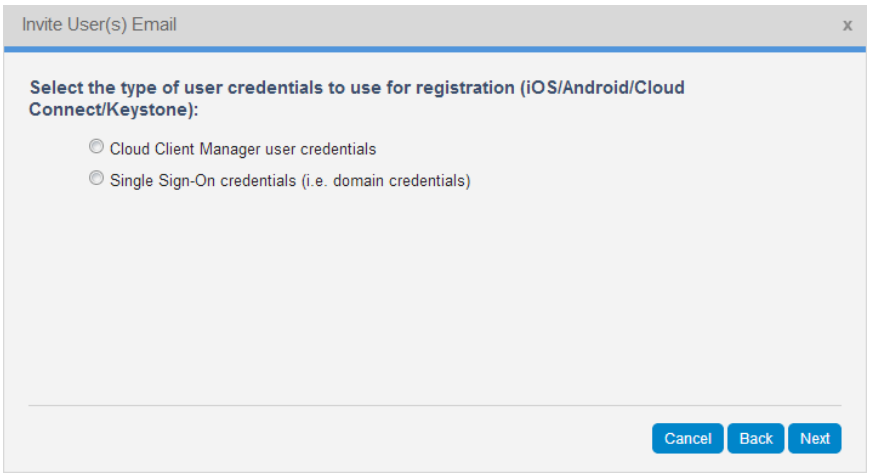
= If user has logged in from PocketCloud app using Cloud Client Manager credentials

b. **Enhancements to email message templates for user invitations**: New email invite wizard for sending email instructions to users for device registration.

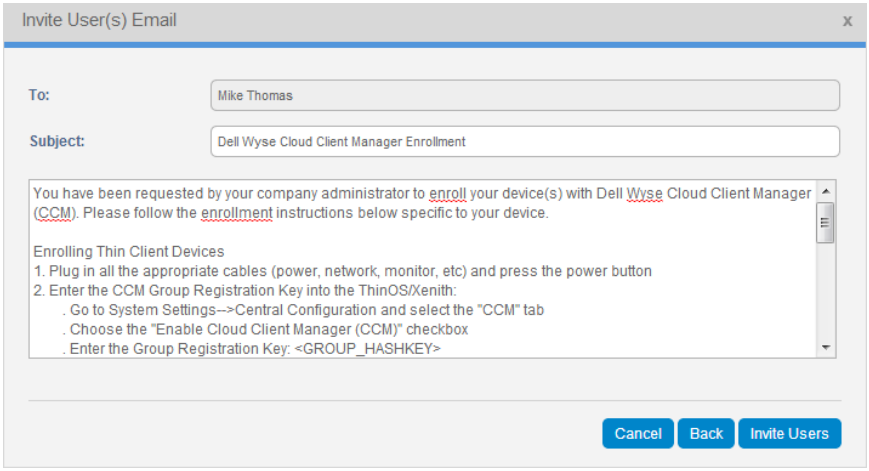
Portal Administrators can select the device types they would like to send a registration invitation for.



For devices that require user registration (iOS, Android, Cloud Connect) the wizard will then provide option to request user to use either Cloud Client Manager credentials or domain credentials.



Prior to sending to user(s), the Portal Administrator can update the email subject and message.


Invite User(s) Email
x
To:
Mike Thomas
Subject:
Dell Wyse Cloud Client Manager Enrollment
You have been requested by your company administrator to enroll your device(s) with Dell Wyse Cloud Client Manager (CCM). Please follow the enrollment instructions below specific to your device.
Enrolling Thin Client Devices
1. Plug in all the appropriate cables (power, network, monitor, etc) and press the power button
2. Enter the CCM Group Registration Key into the ThinOS/Xenith:
. Go to System Settings-->Central Configuration and select the "CCM" tab
. Choose the "Enable Cloud Client Manager (CCM)" checkbox
. Enter the Group Registration Key: <GROUP_HASHKEY>
Cancel
Back
Invite Users

- ## Supported Devices

Thin Client Requirements

- **Supported Devices:** Thin Clients supported include:
  - C00X (Wyse Xenith) running firmware 2.0_021 or later (**recommended 2.0_026 or later)**
  - R00LX (Wyse Xenith Pro) running firmware 2.0_021 or later (**recommended 2.0_026 or later)**
  - T00X (Xenith 2) running firmware 2.0_021 or later **(recommended 2.0_026 or later)**
  - C10LE running firmware ThinOS 7.1_207 or later(**recommended 8.0_105 Hotfix or later)**
  - R10L running firmware ThinOS 7.1_207 or later (**recommended 8.0_105 Hotfix or later)**
  - T10 running firmware ThinOS 7.1_207 or later (**recommended 8.0_105 Hotfix or later)**
  - D10D running firmware ThinOS 7.1_207 or later (**recommended 8.0_105 Hotfix or later)**
  - D10DP running firmware ThinOS 8.0_117 or later

  ***Refer to CCM support site for updates on supported devices:
  https://support.cloudclientmanager.com/entries/22579541

  For supported thin clients running earlier versions, a firmware update is required to enable Cloud Client Manager connectivity. Updates can be downloaded from the Wyse Self-Service Center at: http://support.wyse.com/selfservice.html

  IMPORTANT: You must use your *ThinOS Maintenance* (you should have received an email from Wyse or your reseller with full instructions) to obtain available firmware updates (if you did not receive this email, contact your reseller). If unfamiliar with updating firmware on Wyse ThinOS cloud clients, refer to Wyse Knowledge Base Solution #**10566** (go to Wyse Knowledge Base at http://www.wyse.com/kb and search for **10566**).

- **Connectivity Requirements:**
  - TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com

iOS Requirements

- **Supported Devices:**
  - iPhone, iPad, iPod Touch devices running iOS Version 5.x and later

- **Connectivity Requirements:**
  - TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 80 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 8443 (outbound) to us1-mdm.cloudclientmanager.com
  - TCP port 5223 (outbound) - for Apple APNS

- **MDM Certificate Requirements:**
  - A Mobile Device Management (MDM) Apple Push Notification Service (APNs) certificate is required for iOS device management - this requires an Apple ID. As the Apple ID account will be linked to the APNs certificate, which must be renewed annually, a corporate Apple ID account should be used and not a personal one

Android Requirements

- **Supported Devices:**
  i. Devices running Android Version 2.3 and later

- **Connectivity Requirements:**
  i. TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  ii. TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com

On Premises Gateway Requirements

- **Supported Devices:**
  i. Windows machine running Windows 7, Windows 8
  ii. Minimum CPU requirements: 1 GHz (x86 processor) or 1.4 GHz (x64 processor)
  iii. Minimum available RAM: 1 GB
  iv. Minimum Disk Space: 2 GB available (for install and maintaining service operation)

- **Connectivity Requirements:**
  i. TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  ii. TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com

  NOTE: The On Premises Gateway must be installed on a server within the DMZ externally accessible, and the fully qualified domain name (FQDN) of the server must be registered in public DNS.

Windows Agent Requirements

- **Connectivity Requirements:**
  - TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com
- **OS Requirements:**

Windows Version	OS Architecture	
	32-bits	64 - bits
Windows 8 / Pro / Enterprise	YES	YES
Windows 7 Starter / Home Basic / Home Premium / Professional / Enterprise / Ultimate – Service Pack 1	YES	YES
Windows Server 2012 Standard / Essential / Datacenter / Foundation – Service Pack 1	YES	YES
Windows Web Server 2008 R2 – Service Pack 1	**N/A**	YES
Windows Storage Server 2008 R2 – Service Pack 1	**N/A**	YES
Windows Server 2008 R2 Standard Ed. / Enterprise Ed. / Datacenter Ed. – Service Pack 1	**N/A**	YES
Windows Server 2008 R2 for Itanium-based Systems - Service Pack 1	**N/A**	YES
Windows HPC Server 2008 R2 for high Performance supercomputers - Service Pack 1	**N/A**	YES
Windows Server 2008 R2 Foundation - Service Pack 1	**N/A**	YES
Windows Web Server 2008	YES	YES

Windows Server 2008 Standard Edition (Microsoft Windows NT 6.0 6002 Service Pack 2)	YES	YES
Windows Server 2008 Enterprise Edition (Microsoft Windows NT 6.0 6001 Service Pack 1)	YES	YES
Windows Server 2008 Datacenter Edition	YES	YES
Windows Storage Server 2008	YES	YES
Windows Small Business Server 2008	YES	YES
Windows Essential Business Server 2008	YES	YES
Windows Server 2008 for Itanium-based Systems	YES	YES
Windows HPC Server 2008 for high Performance supercomputers	YES	YES
Windows Server Foundation 2008	YES	YES

- **Known Issues**

STR-678	iOS registration fails if re-registering within 30 seconds
STR-842	Some iOS/Android sub-options at lower policy level not affected by changes to parent options at higher policy level
STR-1148	Android device prompts for app install for installed System apps
STR-1173	Remove certificate for iOS payload fails unless linked payload is removed
STR-1409	Picture taken from the Android back camera compressed on Agent display (correct on server)
STR-1497	iOS Webclip uploaded image truncated in IE8 in CCM console
STR-2335	User/Device Details summary view not displaying some iOS settings when payload configured at higher level is saved with default settings at user/device level.
STR-2414	Event missing when removing device-level exception payloads
STR-2449	Cannot deactivate AD user missing email address
STR-2489	Apps installed from App Store not tagged as “not managed” in CCM Agent when user cancels the app install request on device
STR-2729	During Thin Client registration, in specific scenario device shows as compliant even if configuration could not be loaded.
STR-3009	In Thin Client system information, the “802.1X Auth” field may report N/A when invalid characters received
STR-3137	User prompted to reinstall enterprise app when changing group and app assigned to both groups (iOS)
STR-3598	Prompt for Registration Key with “Default Policy Group” for PC Agent download (IE 8 only)

- **Issues resolved in this release**

STR-2712	Some Android devices displaying app identifier instead of app name in Restrictions message
STR-3218	Change Thin Client visual experience between Classic Desktop and Zero Launchpad from Advanced payload doesn't trigger automatic restart
STR-3301	Thin Client reboots when it has DesktopColorDepth setting in both Display and Advanced payload but with different values
STR-3302	Some Thin Client payloads (Remote Connections and Security) take precedence over Advanced payload
STR-3346	Starter Tenant issue editing a user.
STR-3461	CCM Agent reporting incorrect category for apps rejected on device and subsequently installed directly from app store
STR-3473	Admin with “Global Viewer” role cannot access "Export to CSV" unless granted privileges to another operation
STR-3549	Incorrect image shown for D10 Thin Client in details page
STR-3590	PC Agent download button disabled if selecting a group after selecting another group that has no registration key assigned. Workaround: Refresh Page
STR-3604	“Remove App” command sometimes generated for user installed app (Android)

"R3" Release (October 10, 2013)

- **Release Overview**

This Cloud Client Manager release introduces cloud-based Windows software providing asset visibility, remote troubleshooting and management, and the ability to send remote commands to Windows devices. The Windows agent (currently in Tech preview) can be easily downloaded and installed on users' Windows devices and registered with Cloud Client Manager within a few minutes.

Other features introduced in this release include enhancements for iOS 7 device management, the ability to send customized messages to mobile devices, a new license subscription page, and a new help page with tips to assist with registering the various devices types supported by Cloud Client Manager.

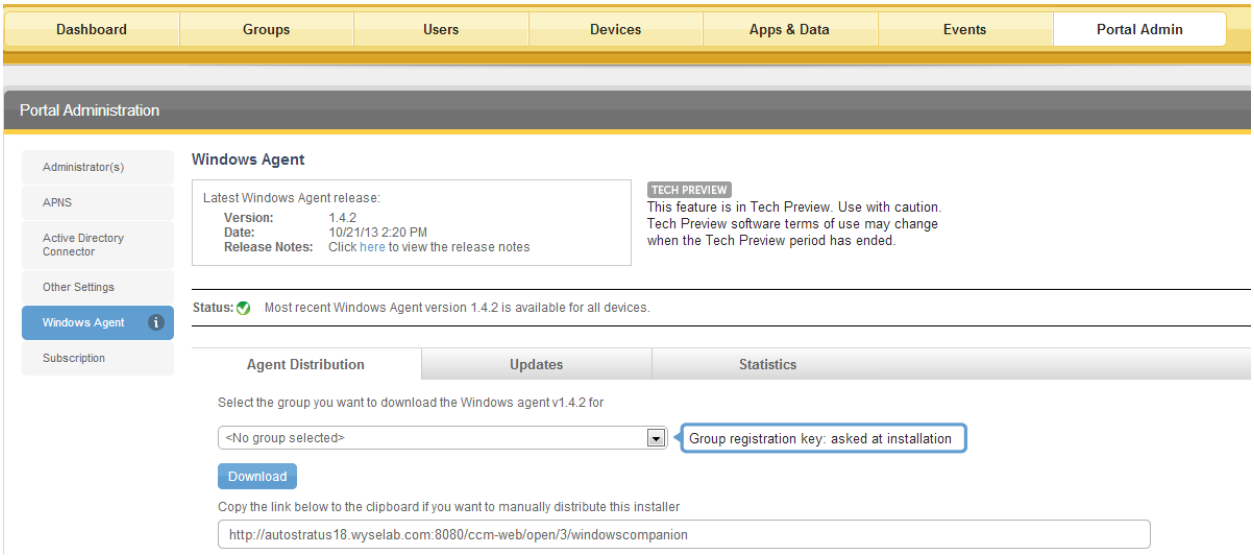
Highlights of this release:

- **New CCM Windows Agent (Tech Preview)**
  - Simple and efficient way to manage Windows devices
  - Easy installation and both automatic and manual updates are supported
  - Enhanced visibility into device's system information and vitals: HW details, OS details, network details, security settings, antivirus settings, windows firewall settings
  - Statistics available for Device inventory
- **Windows Device Management from CCM server**
  - Send remote commands to Windows devices
  - Troubleshooting tools: view/stop running processes, view/stop/restart running services; request screenshot functionality
- **Enhancements for iOS 7 support**
  - Support for new iOS 7 "Open-In" restrictions, device restrictions and new queries (supported on devices running iOS 7+)
- **Send Message to Devices**
  - Send customized message to Android, iOS, Dell Wyse Cloud Connect, and Windows devices (iOS requires Cloud Client Manager Agent)
- **Platform Enhancements**
  - Subscription Info page to review purchased, in-use, and remaining licenses from portal, as well as license expiration date
  - "How to Add a Device" page to assist with device registration

- **New Features Details**

2. Downloading/updating the Windows Agent (Tech Preview)

a) A new "**Windows Agent**" page is available from **Portal Admin** tab


Dashboard
Groups
Users
Devices
Apps & Data
Events
Portal Admin
Portal Administration
Administrator(s)
APNS
Active Directory Connector
Other Settings
Windows Agent
Subscription
Windows Agent
Latest Windows Agent release:
Version: 1.4.2
Date: 10/21/13 2:20 PM
Release Notes: Click here to view the release notes
TECH PREVIEW
This feature is in Tech Preview. Use with caution. Tech Preview software terms of use may change when the Tech Preview period has ended.
Status: Most recent Windows Agent version 1.4.2 is available for all devices.
Agent Distribution
Updates
Statistics
Select the group you want to download the Windows agent v1.4.2 for
<No group selected>
Group registration key: asked at installation
Download
Copy the link below to the clipboard if you want to manually distribute this installer
http://autostratus18.wyselab.com:8080/ccm-web/open/3/windowscompanion

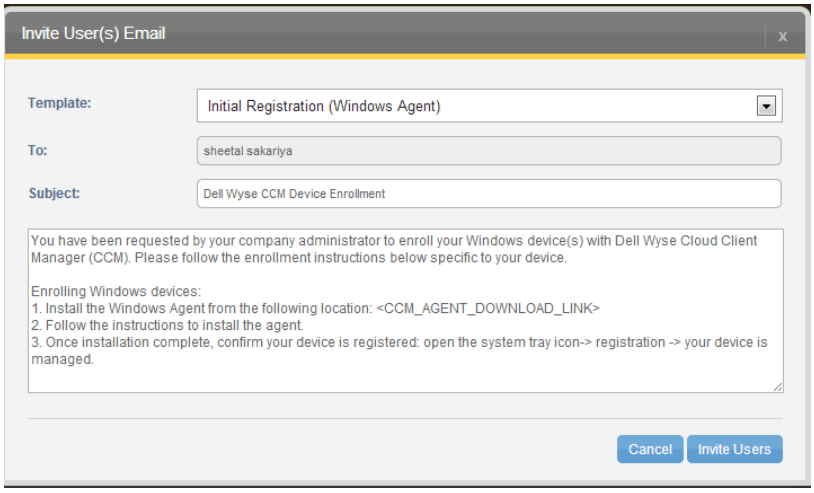
b) This page shows the version number and release date of latest Windows Agent, and a link to the release notes.

c) There are 3 main tabs on this page: **Agent Distribution**, **Updates**, and **Statistics**

d) **Agent Distribution** tab: The user may download the generic Windows agent app or choose a group from the dropdown menu, and then download the customized Windows agent app. The generic agent will require the user to enter group registration key at installation. The customized agent will not require a group registration key.

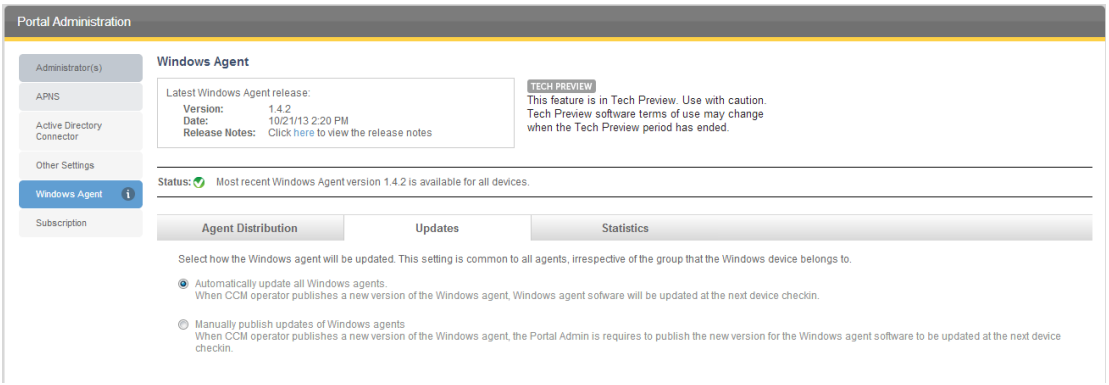
Alternatively the user may also copy the link at the bottom of the page and email the link to others to download/install the Windows agent application.

A third way to download the agent is invite users through email as shown below:

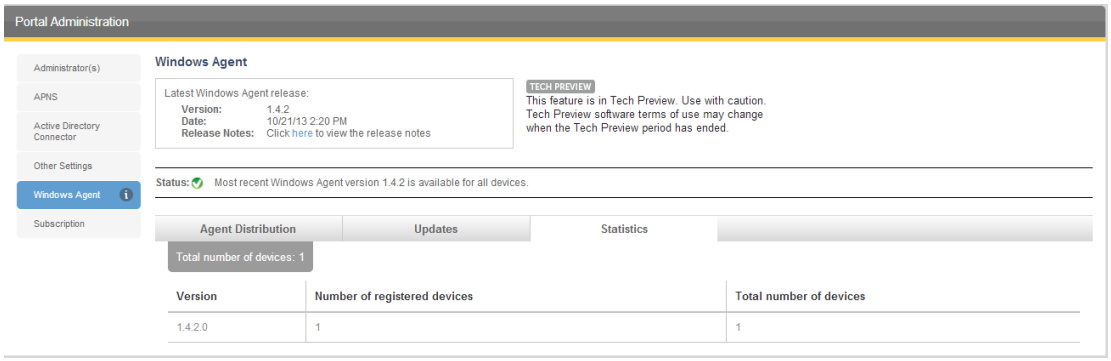

Invite User(s) Email
x
Template:
Initial Registration (Windows Agent)
To:
sheetal sakariya
Subject:
Dell Wyse CCM Device Enrollment
You have been requested by your company administrator to enroll your Windows device(s) with Dell Wyse Cloud Client Manager (CCM). Please follow the enrollment instructions below specific to your device.
Enrolling Windows devices:
1. Install the Windows Agent from the following location: <CCM_AGENT_DOWNLOAD_LINK>
2. Follow the instructions to install the agent.
3. Once installation complete, confirm your device is registered: open the system tray icon-> registration -> your device is managed.
Cancel
Invite Users

e) **Updates** tab: the user can choose the automatic option or a manual option. Automatic updates will be published to the user as soon as the stratus operator publishes the updates.

Manual updates will be published to the user after the IT admin clicks on this option and clicks on the "**Publish v X.Y.Z**" button.


Portal Administration
Administrator(s)
APNS
Active Directory Connector
Other Settings
Windows Agent
Subscription
Windows Agent
Latest Windows Agent release:
Version: 1.4.2
Date: 10/21/13 2:20 PM
Release Notes: Click here to view the release notes
TECH PREVIEW
This feature is in Tech Preview. Use with caution.
Tech Preview software terms of use may change when the Tech Preview period has ended.
Status: Most recent Windows Agent version 1.4.2 is available for all devices.
Agent Distribution
Updates
Statistics
Select how the Windows agent will be updated. This setting is common to all agents, irrespective of the group that the Windows device belongs to.
Automatically update all Windows agents.
When CCM operator publishes a new version of the Windows agent, Windows agent sofware will be updated at the next device checkin.
Manually publish updates of Windows agents
When CCM operator publishes a new version of the Windows agent, the Portal Admin is requires to publish the new version for the Windows agent software to be updated at the next device checkin.

f) **Statistics** tab: this information will provide a quick inventory snapshot - number of registered Windows devices, versions installed, and the total number of Windows devices that exist.



3. Installing Windows Agent

a) After downloading, user runs the installation file (.msi) in order to register Windows Agent to CCM server.

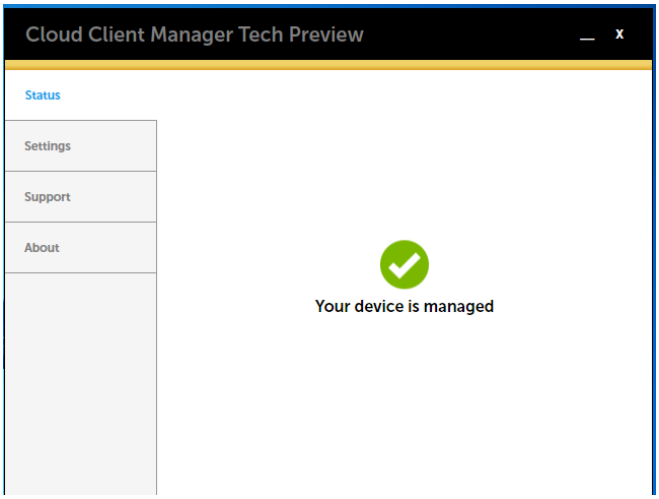
b) The user can select either to "Install Now" or change the installation path, if desired.

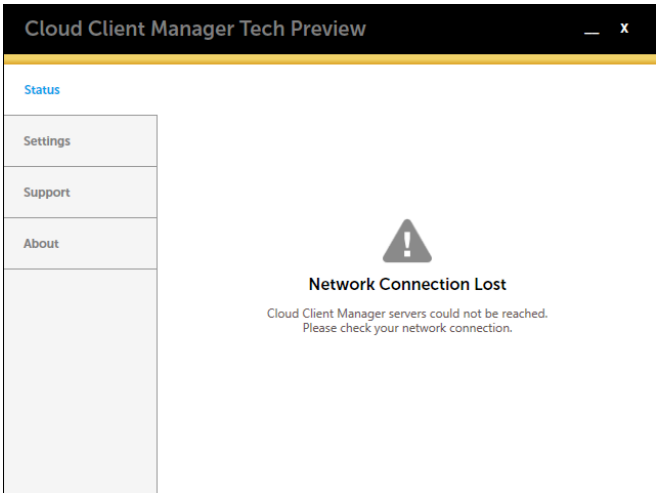
c) The user will be asked to confirm that changes will occur on the computer due to a program installation. Once they click "**Yes**", installation will be complete.

d) There will be a confirmation message that the installation was successful. Click "**Finish**" to complete the installation setup.

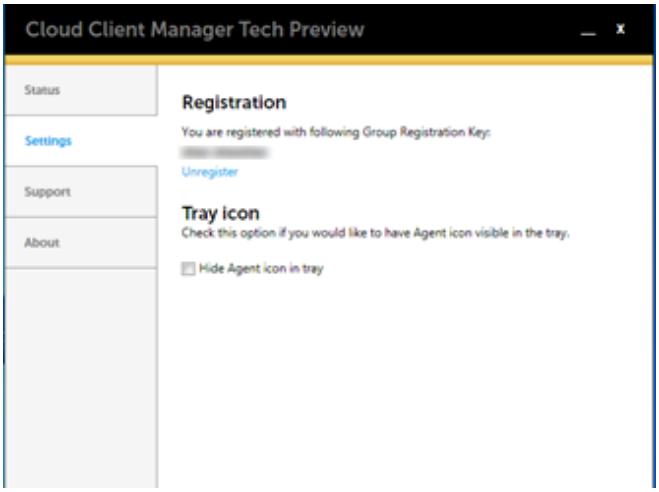
e) There are 4 tabs within the CCM Windows agent: **Status, Settings, Support, About**

- **Status**: will show connection status to internet/CCM server. Green means that you are connected. Grey (with an exclamation mark) generally means device has lost Internet connectivity.

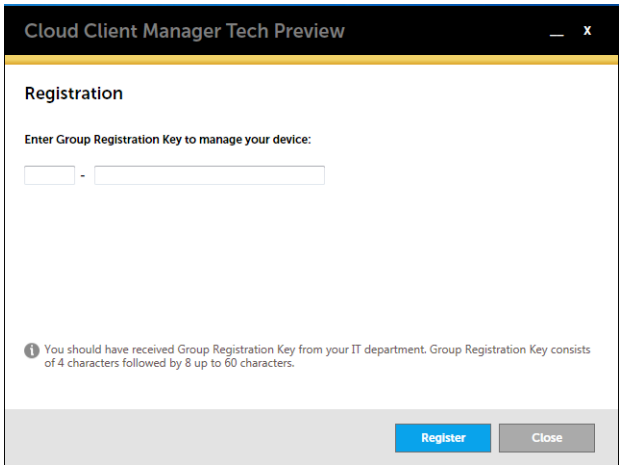




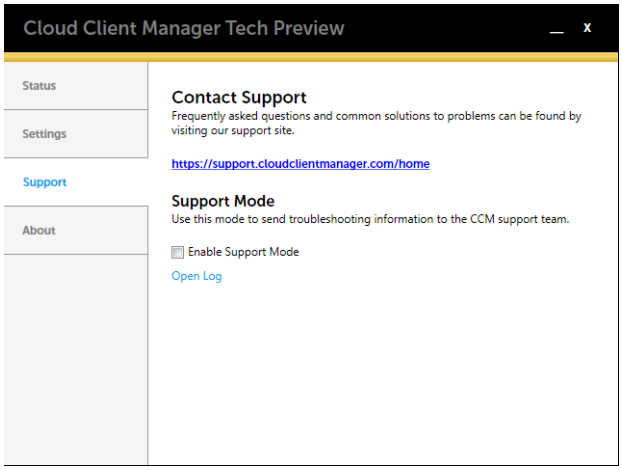
- **Settings:** The user will be able to register/unregister his device with a group registration key (provided by his admin). Also, the user can choose to hide/unhide the CCM tray icon.



If user presses the **Unregister** button, they will be prompted to confirm unregistering the Windows agent from CCM server. Re-registration requires a valid group registration key.


Cloud Client Manager Tech Preview
Registration
Enter Group Registration Key to manage your device:
You should have received Group Registration Key from your IT department. Group Registration Key consists of 4 characters followed by 8 up to 60 characters.
Register
Close

- **Support**: If "**Enable Support Mode**" is checked, agent logging is enabled. Log files are stored in the installation folder and can be easily emailed to the IT Admins for troubleshooting. The "**Open Log**" button opens the folder where the logs are stored.



- **About:** Displays the EULA and the Windows Agent version.

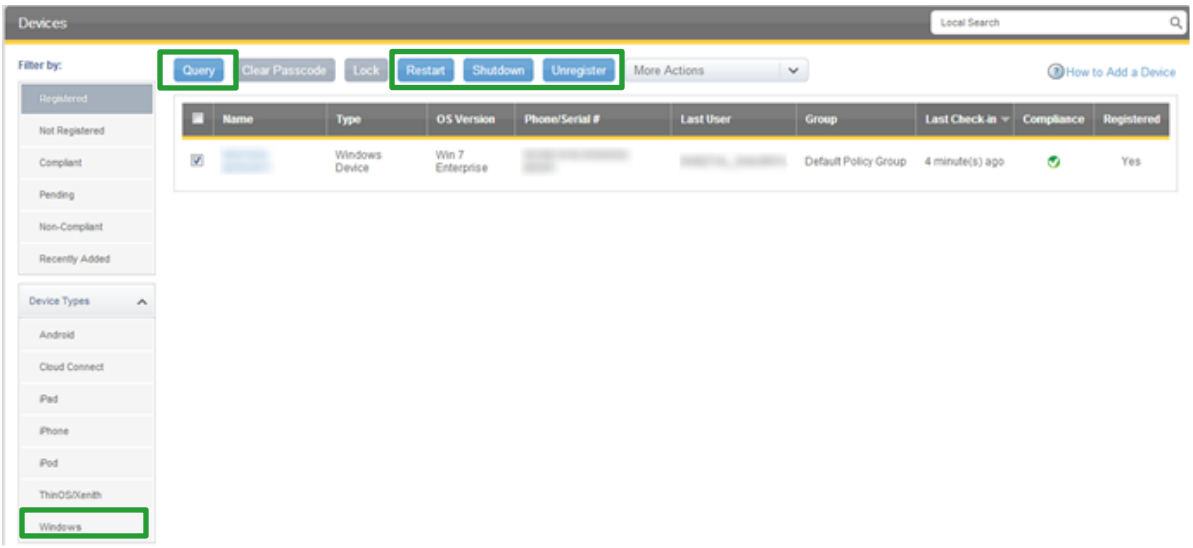
Cloud Client Manager Tech Preview
Status
Settings
Support
About
Cloud Client Manager Windows Agent
Version: 1.4.2.0
http://www.wyse.com/ccm
License Agreement
Wyse
3rd Party
End User License Agreement - Type S
This is a legal agreement ("Agreement") between you, the user, and Dell Products L.P., a Texas limited partnership, or Dell Global B.V. (Singapore Branch), a Singapore branch of a company incorporated in The Netherlands with limited liability, on behalf of itself, Dell Inc., and Dell Inc.'s other subsidiaries and affiliates (together "Dell"). This Agreement covers all software ("Software") and any upgrades, updates, patches, hotfixes, modules, routines, feature enhancements and additional versions of the Software that replace or supplement the original Software (collectively "Updates") distributed by Dell unless there is a separate license agreement between you and the manufacturer or owner of the Software or Update. If there is no separate license agreement

4. Devices Page UI Changes

a) Added “Windows” to **Device Types** filter.

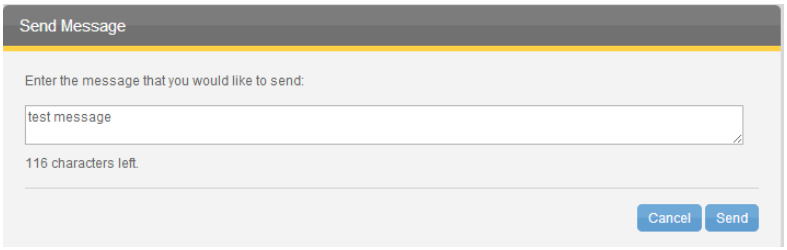
b) New commands for Windows Devices: **Query**, **Restart**, **Shutdown**, **Unregister**.

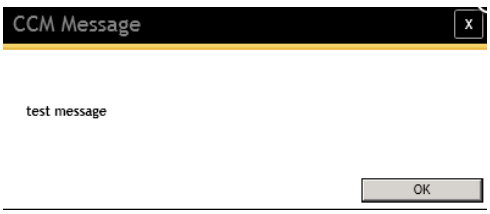
- **Query**: Requests Windows Agent to update CCM console with updated device information.
- **Restart** will reboot the device with a warning message.
- **Shutdown** will shutdown the device
- **Unregister** will unregister the device from CCM server Device will no longer be managed by the CCM cloud based service.



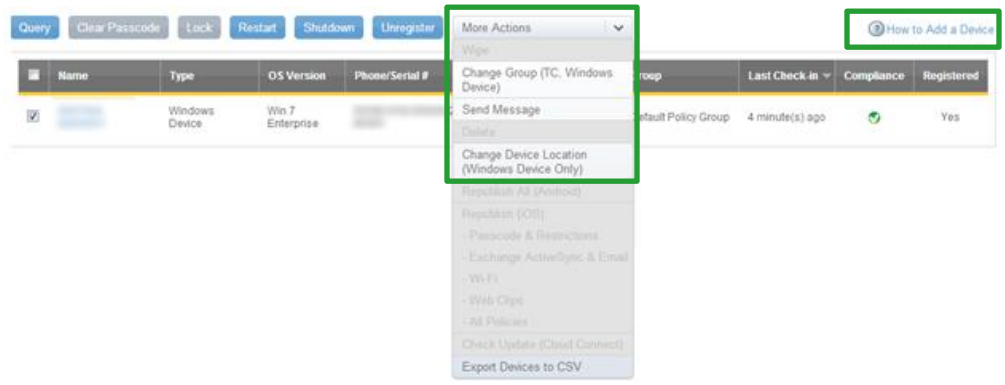
c) Commands under more actions: **Send Message**, **Change Group**, **Change Device Location**.

- **Send Message** will allow IT admins to send messages to the device. Below is the example of the message that IT admins can send and user will receive on his device:

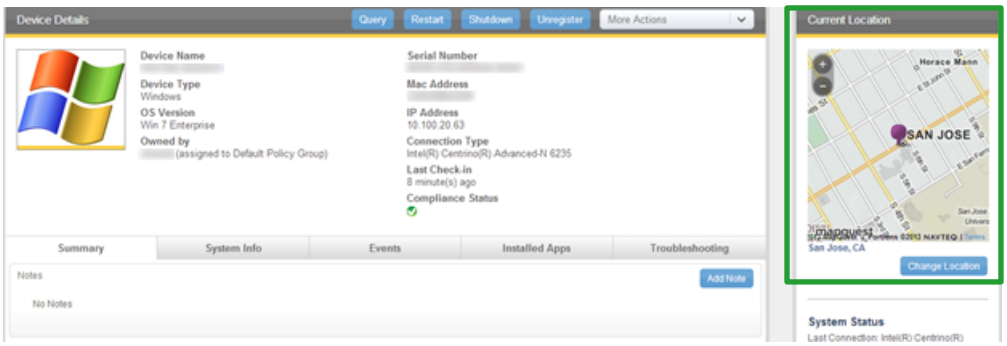




- **Change Group** will allow IT admins to change group of the device (e.g. Change a group from **Engineering** group to **Sales** group)



- **Change Device Location** will allow IT admins to enter a location of the device. Location will be updated on the device details page as shown below

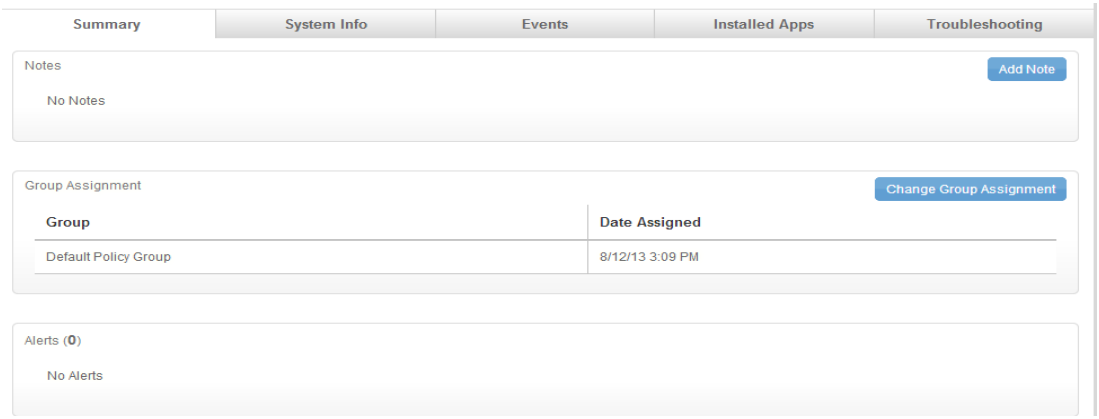


5. Device Details Page UI

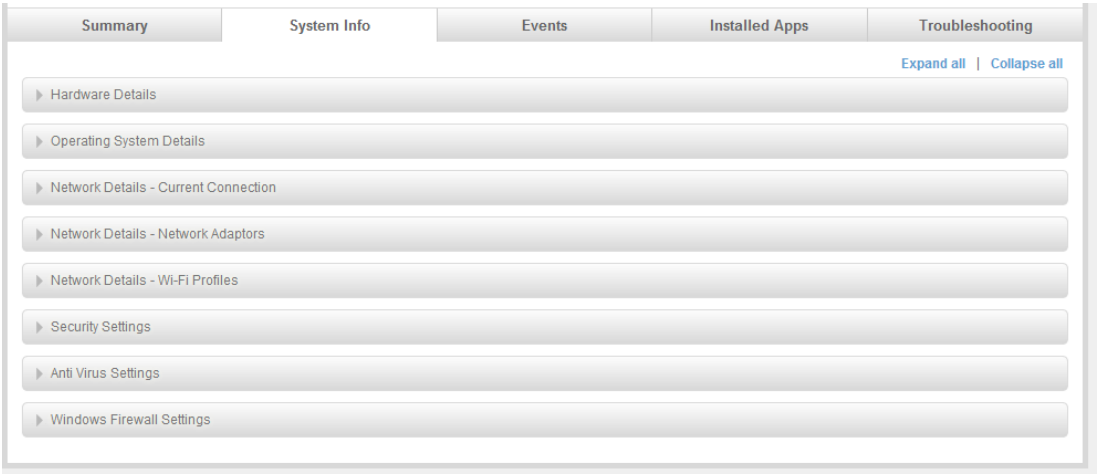
a) Once a Windows device is selected on the **Devices** page, a **Device Details** page will show like below for the device. The top part of this page contains a quick snapshot of basic information about the device: Device name, Device type, OS version, Owner, Serial Number, Last Check-In, and Compliance Status.

b) There are 5 new tabs created under the device details page:

- **Summary**: The summary tab will contain notes that are specific for that device. As an admin, you can also change group assignment at this place. And it will provide a list of alerts for the device



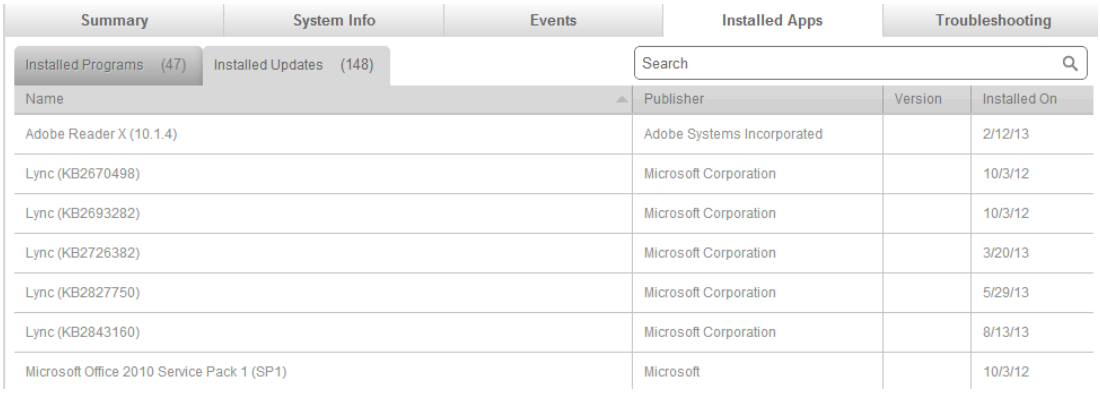
- **System info**: The system info tab will retrieve the vital information about the device. The Windows agent installed on the device will pull this information from the device, and report it to CCM server. This information is very useful to understand basic HW details, operation system details, network details, security settings, antivirus settings, and Windows firewall settings. The admin can expand/collapse the below categories to see a particular category.



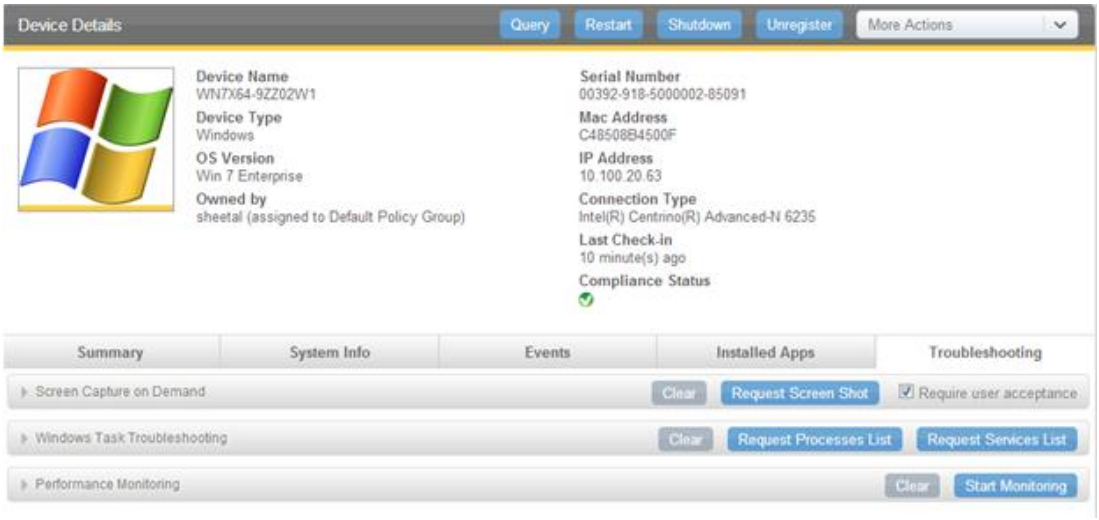
- **Events**: The events tab will report all events that are particular to that device. (e.g. registration, unregister, remote commands, etc.), including information regarding status of the command (**Successful**, **In-Progress**, **Pending**, **Failed**).

- **Installed Apps**: The installed apps tab contains 2 tabs. **Installed Programs** lists all the installed programs on the device and includes the publisher, version and installed date. This info is helpful for the IT admins to compare list of installed programs to company policy. Installed updates tab gives a complete list of already installed updates – other columns include publisher name, version, and installed on date. The IT admin will be able to sort the columns in installed program/updates tabs.

- **Search field:** The IT admin is also able to search a certain application by name if you just type the name in the search field under installed programs and installed updates tab.



- **Troubleshooting**: The **Troubleshooting** tab is primarily designed to help IT admins remotely troubleshoot issues. Administrators are able to check for system info and verify the device and security settings. The **Troubleshooting** tab offers three support tools:



- **Screen Capture on Demand**: the IT admin may request a screenshot (with/without user's knowledge/permission).
- **Windows Task Troubleshooting**: Administrator may request from device the Windows Processes and Services list to see current status on Windows device. Admin may also choose to stop an application remotely by selecting an application and pressing the **End** button, or to remotely **Stop** or **Restart** a running service.
- **Performance Monitoring**: By clicking "**Start Mirroring**" Administrators gain visibility into the average memory and CPU usage over previous minute.

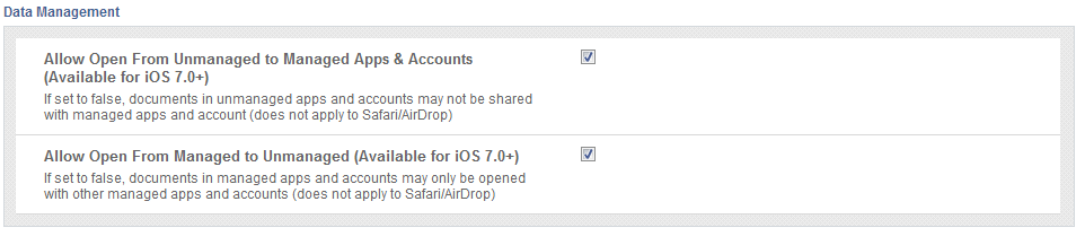
6. Enhancements for iOS 7 support

The following features have been added for enhanced support of iOS devices. These features are not available on pre-iOS 7 devices:

a) New Data Management Restrictions (from iOS policy > **Restrictions** settings):

i. **Open From Unmanaged to Managed Apps & Accounts**: Option to prevent documents in unmanaged apps and accounts to be shared with managed apps and account. Managed apps are those that are managed by CCM [**Requires Pro Tier**]. **Note**: Does not apply to Safari/AirDrop

ii. **Open From Managed to Unmanaged**: Option to prevent documents in managed apps and accounts to only be opened with other managed apps and accounts. Managed apps are those that are managed by CCM [**Requires Pro Tier**]. **Note**: Does not apply to Safari/AirDrop

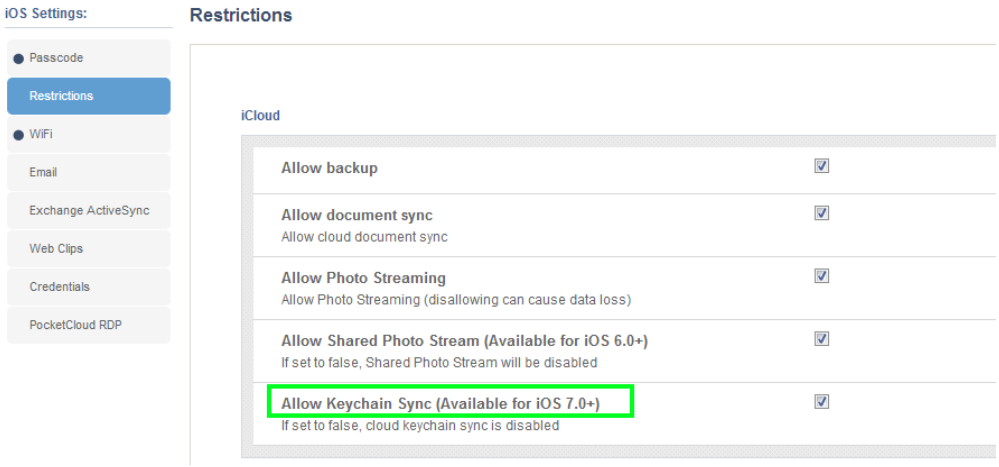

Data Management
Allow Open From Unmanaged to Managed Apps & Accounts (Available for iOS 7.0+)
If set to false, documents in unmanaged apps and accounts may not be shared with managed apps and account (does not apply to Safari/AirDrop)
Allow Open From Managed to Unmanaged (Available for iOS 7.0+)
If set to false, documents in managed apps and accounts may only be opened with other managed apps and accounts (does not apply to Safari/AirDrop)

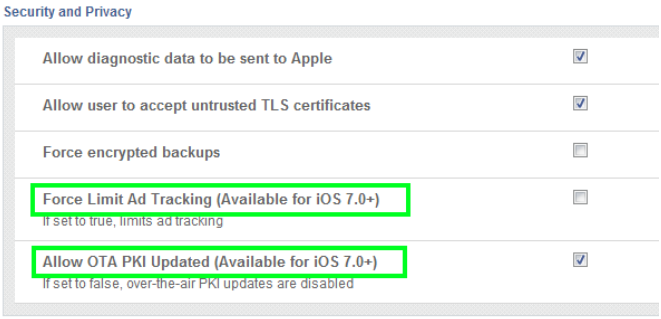
b) New Device Restrictions (from iOS policy > **Restrictions** settings):

i. **Keychain Sync** : Option to disable iCloud keychain sync

ii. **Force Limit Ad Tracking**: Option to limit ad tracking

iii. **OTA PKI Updates**: Option to disable over-the-air PKI updates




Security and Privacy
Allow diagnostic data to be sent to Apple
Allow user to accept untrusted TLS certificates
Force encrypted backups
Force Limit Ad Tracking (Available for iOS 7.0+)
If set to true, limits ad tracking
Allow OTA PKI Updated (Available for iOS 7.0+)
If set to false, over-the-air PKI updates are disabled

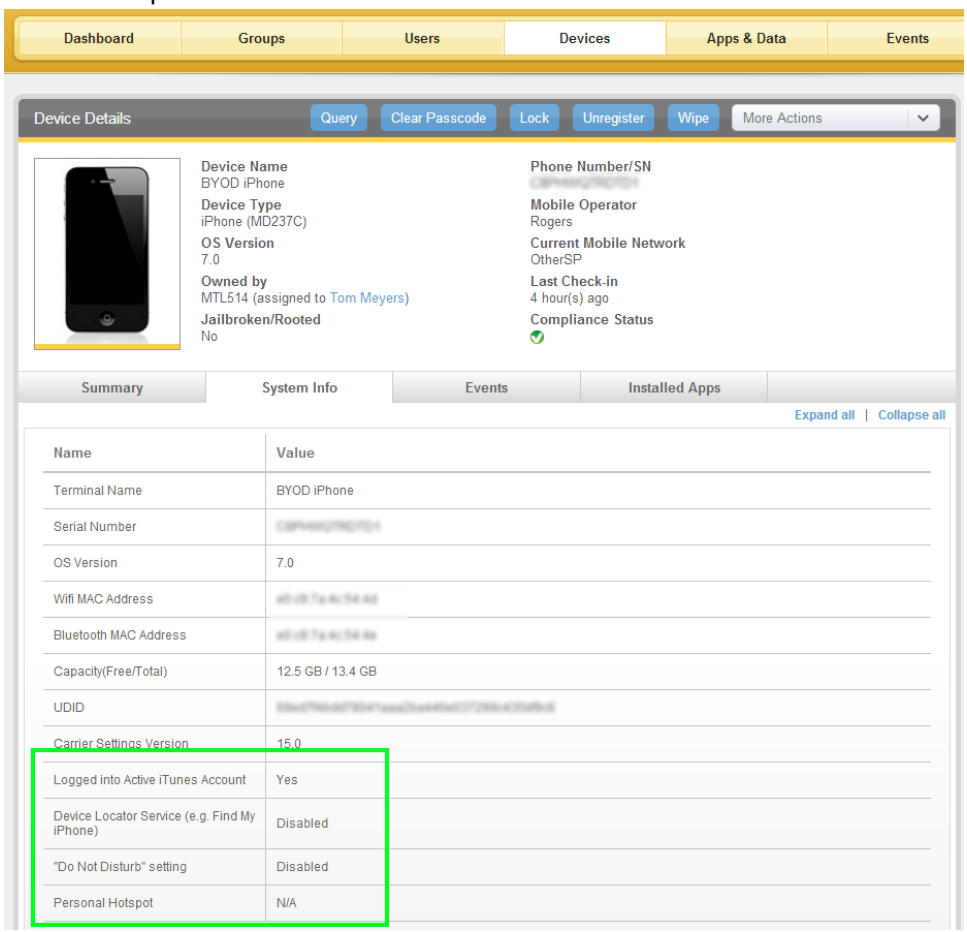
c) New device information available from device queries:

i. **Logged into Active iTunes Account:** indicates whether or not user is logged into an active iTunes account

ii. **Device Locator Service:** indicates whether or not a device locater service (e.g. Find My iPhone) is enabled on device

iii. **"Do Not Disturb" Setting:** indicates whether or not "Do Not Disturb" setting is enabled on device

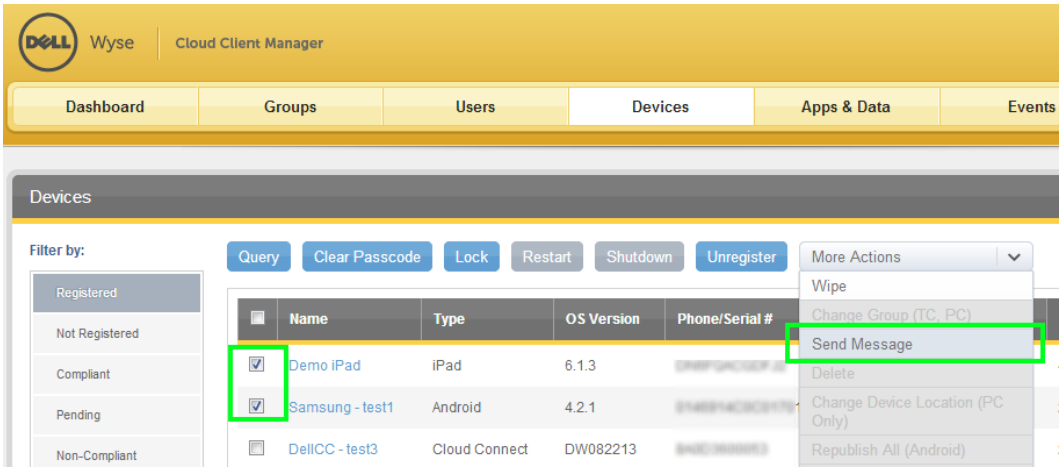
iv. **Personal Hotspot:** indicates whether or not device is being used as a personal hotspot



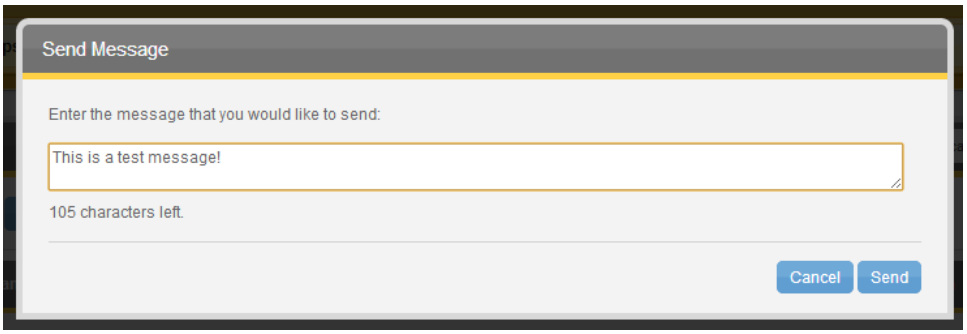
7. Send Customized Message

New option to send a customized message to devices. The message must be 128 characters or less. This option is supported on Android, Dell Wyse Cloud Connect, and Windows PC devices. It is also supported for iOS if the device has the **Cloud Client Manager Agent** installed on it.

To send a customized message, select one more devices from the **Devices** page and click **More Actions > Send Message**.



In the **Send Message** window enter the desired message (up to 128 characters) and click the **Send** button. Message will appear on the device as a notification.

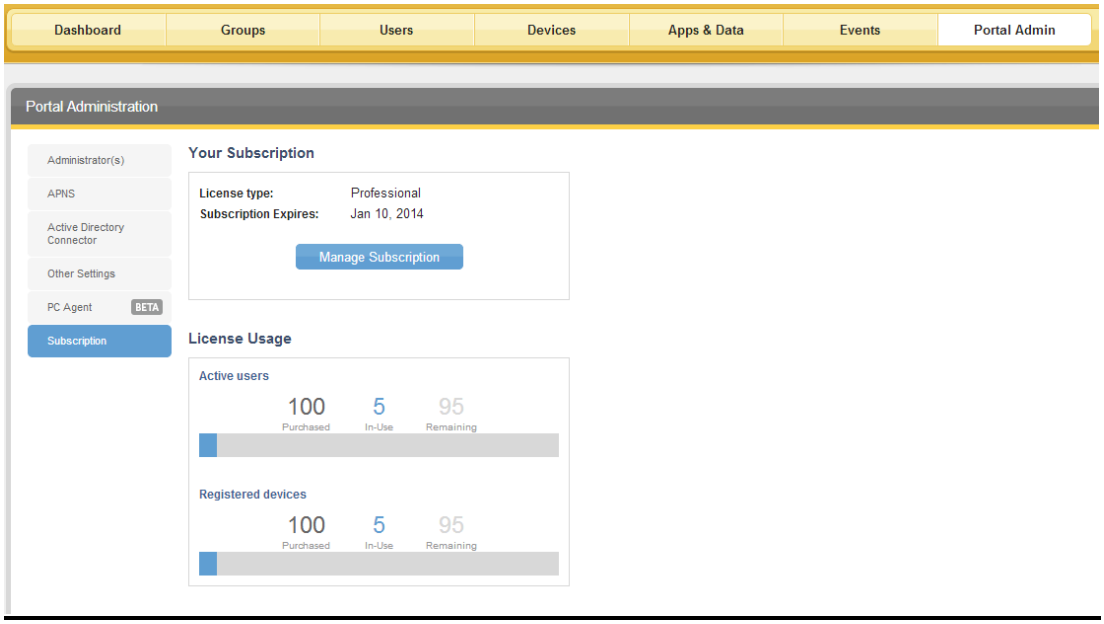


8. Platform Enhancements

a) Subscription Information

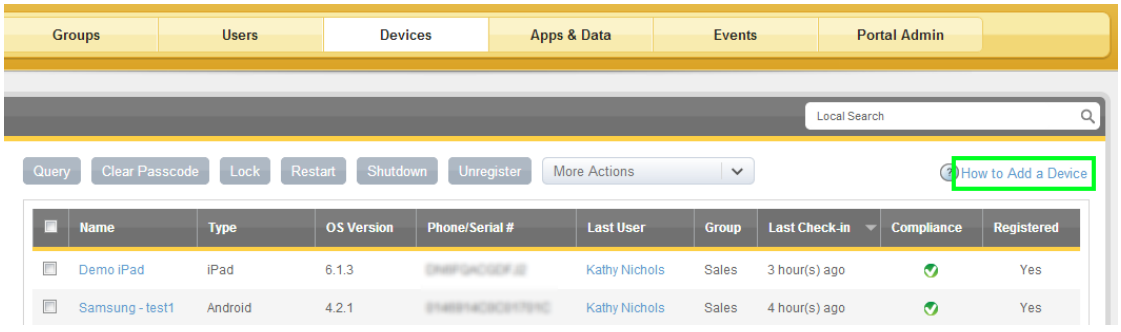
New **Your Subscription** page available from **Portal Admin > Subscription**. From this page the number of purchased, in-use and remaining device and user licenses may be viewed. Additionally, may now also review the subscription expiration date. Alerts have also been added when the license is set to expire within 30 days (at login).

There is also a "**Manage Subscription**" button which will open a new webpage to login to the CCM Billing portal.



b) "How to Add a Device" feature

New "**How to Add a Device**" link available from **Devices** page. This provides a quick overview with tips and helpful information on how to register various device types: Thin Clients, Android, iOS, Dell Wyse Cloud Connect, and Windows PCs.



How to Add a Device
PC
Mobile Device
Thin Client
Cloud Connect
How to Add a Mobile Device
1
Install Cloud Client Manager Agent app on the device.
You can get the app on:
Available on the App Store
Get it on Google play
2
Sign in with user credentials.
username
*****
To send an email that includes the app download link and credentials for users to self-enroll their mobile devices, use the email templates available from the "Invite User(s)" option from the Users page.
Close

- ## Supported Devices

Thin Client Requirements

- **Supported Devices:** Thin Clients supported include:
  - C00X (Wyse Xenith) running firmware 2.0_021 or later (**recommended 2.0_026 or later)**
  - R00LX (Wyse Xenith Pro) running firmware 2.0_021 or later (**recommended 2.0_026 or later)**
  - T00X (Xenith 2) running firmware 2.0_021 or later **(recommended 2.0_026 or later)**
  - C10LE running firmware ThinOS 7.1_207 or later (**recommended 8.0_037 or later)**
  - R10L running firmware ThinOS 7.1_207 or later (**recommended 8.0_037 or later)**
  - T10 running firmware ThinOS 7.1_207 or later (**recommended 8.0_037 or later)**
  - D10D running firmware ThinOS 7.1_207 or later (**recommended 8.0_037 or later)**

  For supported thin clients running earlier versions, a firmware update is required to enable Cloud Client Manager connectivity. Updates can be downloaded from the Wyse Self-Service Center at: http://support.wyse.com/selfservice.html

  IMPORTANT: You must use your *ThinOS Maintenance* (you should have received an email from Wyse or your reseller with full instructions) to obtain available firmware updates (if you did not receive this email, contact your reseller). If unfamiliar with updating firmware on Wyse ThinOS cloud clients, refer to Wyse Knowledge Base Solution #**10566** (go to Wyse Knowledge Base at http://www.wyse.com/kb and search for **10566**).

- **Connectivity Requirements:**
  - TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com

iOS Requirements

- **Supported Devices:**
  - iPhone, iPad, iPod Touch devices running iOS Version 5.x and later

- **Connectivity Requirements:**
  - TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 80 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 8443 (outbound) to us1-mdm.cloudclientmanager.com
  - TCP port 5223 (outbound) - for Apple APNS

- **MDM Certificate Requirements:**
  - A Mobile Device Management (MDM) Apple Push Notification Service (APNs) certificate is required for iOS device management - this requires an Apple ID. As the Apple ID account will be linked to the APNs certificate, which must be renewed annually, a corporate Apple ID account should be used and not a personal one

Android Requirements

- **Supported Devices:**
  i. Devices running Android Version 2.3 and later

- **Connectivity Requirements:**
  i. TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  ii. TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com

Windows Agent Requirements

- **Connectivity Requirements:**
  - TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com
- **OS Requirements:**

Windows Version	OS Architecture	
	32-bits	64 - bits
Windows 8 / Pro / Enterprise	YES	YES
Windows 7 Starter / Home Basic / Home Premium / Professional / Enterprise / Ultimate – Service Pack 1	YES	YES
Windows Server 2012 Standard / Essential / Datacenter / Foundation – Service Pack 1	YES	YES
Windows Web Server 2008 R2 – Service Pack 1	**N/A**	YES
Windows Storage Server 2008 R2 – Service Pack 1	**N/A**	YES
Windows Server 2008 R2 Standard Ed. / Enterprise Ed. / Datacenter Ed. – Service Pack 1	**N/A**	YES
Windows Server 2008 R2 for Itanium-based Systems - Service Pack 1	**N/A**	YES
Windows HPC Server 2008 R2 for high Performance supercomputers - Service Pack 1	**N/A**	YES
Windows Server 2008 R2 Foundation - Service Pack 1	**N/A**	YES
Windows Web Server 2008	YES	YES
Windows Server 2008 Standard Edition (Microsoft Windows NT 6.0 6002 Service Pack 2)	YES	YES
Windows Server 2008 Enterprise Edition (Microsoft Windows NT 6.0 6001 Service Pack 1)	YES	YES
Windows Server 2008 Datacenter Edition	YES	YES
Windows Storage Server 2008	YES	YES
Windows Small Business Server 2008	YES	YES
Windows Essential Business Server 2008	YES	YES
Windows Server 2008 for Itanium-based Systems	YES	YES
Windows HPC Server 2008 for high Performance supercomputers	YES	YES
Windows Server Foundation 2008	YES	YES

- **Known Issues**

STR-678	iOS registration fails if re-registering within 30 seconds
STR-842	Some iOS/Android sub-options at lower policy level not affected by changes to parent options at higher policy level
STR-1148	Android device prompts for app install for installed System apps
STR-1173	Remove certificate for iOS payload fails unless linked payload is removed
STR-1409	Picture taken from the Android back camera compressed on Agent display (correct on server)
STR-1497	iOS Webclip uploaded image truncated in IE8 in CCM console
STR-2335	User/Device Details summary view not displaying some iOS settings when payload configured at higher level is saved with default settings at user/device level.
STR-2414	Event missing when removing device-level exception payloads
STR-2449	Cannot deactivate AD user missing required user information
STR-2489	Apps installed from App Store not tagged as “not managed” in CCM Agent when user cancels the app install request on device
STR-2552	VPP file name is not cleared if upload is cancelled and reinitiated
STR-2712	Some Android devices displaying app identifier instead of app name in Restrictions message
STR-2729	During Thin Client registration, in specific scenario device shows as compliant even if configuration could not be loaded.
STR-3009	In Thin Client system information, the “802.1X Auth” field may report N/A when invalid characters received
STR-3109	Thin Client will not revert Global Thin Client firmware mapping in case where a device-level exception has been pushed to device and reverted by using “Select Firmware” option. Workaround: Remove policy from device level exception
STR-3137	User prompted to reinstall enterprise app when changing group and app assigned to both groups (iOS)
STR-3590	PC Agent download button disabled if selecting a group after selecting another group that has no registration key assigned. Workaround: Refresh Page
STR-3598	Prompt for Registration Key with “Default Policy Group” for PC Agent download (IE 8)
STR-3604	“Remove App” command sometimes generated for user installed app (Android)

- **Issues resolved in this release**

STR-2786	Changing Android app policy multiple times between mandatory to not managed may cause extra remove application commands
STR-2922	Changing Android policy sometimes requires Republish to push policies
STR-3105	In Dashboard, Devices, User Details, User Invitations, Portal Admin views labels are not updated (“Thin Client” to “ThinOS/Xenith”) for R2 release
STR-3108	Thin Client firmware policy “Skip local firmware check” is ignored if no firmware mappings are configured in CCM policy

"R2A" Release (August 16, 2013)

Release Overview

This release introduces support for Dell Wyse Cloud Connect devices which enable secure cloud access to business and personal content on any TV or monitor. Dell Wyse Cloud Connect devices can be centrally managed with Dell Wyse Cloud Client Manager, for simple and flexible deployment of policies, applications, certificates and device settings.

Highlights of this release:

- **Dell Wyse Cloud Connect Device Management**
  - Support for all existing Cloud Client Manager Android policies - Passcode, Restrictions, Wi-Fi, PocketCloud RDP
  - Lock down access to either a single app ("Kiosk" mode) or a defined list of applications ("LaunchPad" mode)
  - Certificate management
  - Restrict access to Bluetooth and external storage devices
  - Management of devices settings to hide notification area and prevent installation of apps from "Unknown Sources"
  - Configure Administrator Mode password to locally manage device as an administrator
  - Application management including silent install for enterprise (i.e. non Play Store) apps
- **Enterprise App Store**
  - Ability to upload or link to custom in-house apps for iOS and Android
  - Policy management for custom in-house apps (consistent with policies previously available for apps from public App Store and Google Play)
- **Device Inventory Exportable Report**
  - Export to a CSV file the device asset information
- **New Platform Support**
  - Dell Wyse Cloud Connect devices
- **Other**
  - Enhancements for viewing device table (sort by IP address when Thin Client filter is applied)

New Features Details

1. Dell Wyse Cloud Connect Device Management

Cloud Client Manager enables management of Dell Wyse Cloud Connect devices. Devices are registered to Cloud Client Manager during initial device setup with Cloud Client Manager user credentials. For more details on registering Dell Wyse Cloud Connect devices refer to the **Dell Wyse Cloud Connect® Users Guide.**

NOTE: Customers on **Starter Tier** will be able to log into their Cloud Connect devices and manage generic Android settings, but management of specific Cloud Connect settings mentioned in "b,c,d" below requires **Professional Tier.**

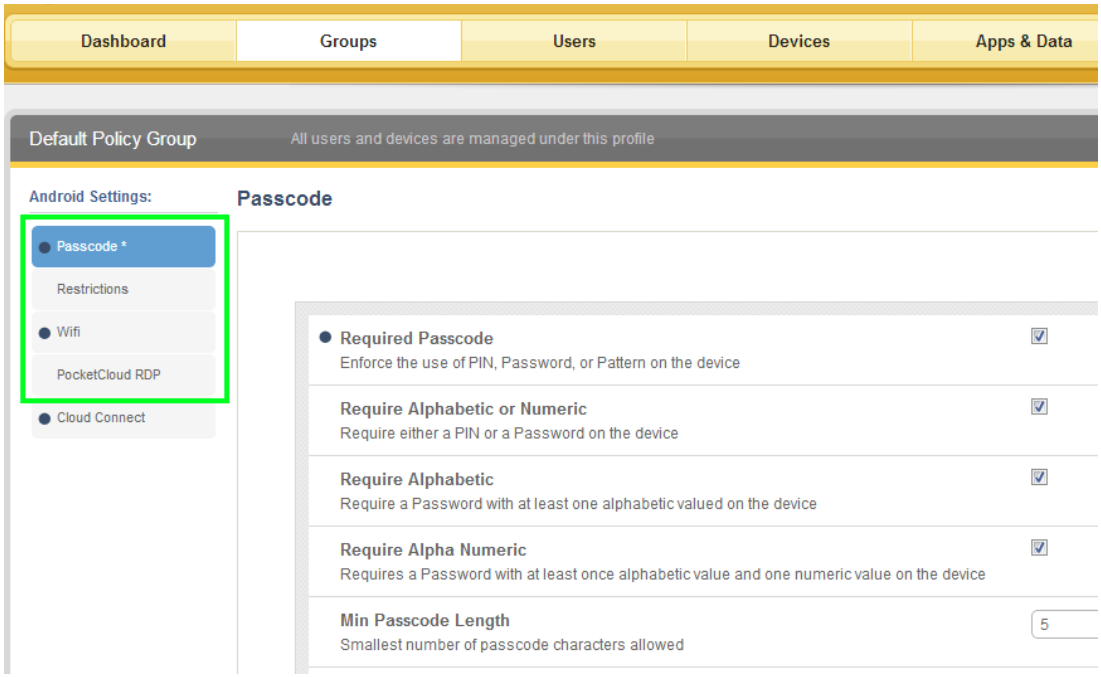
The supported Dell Wyse Cloud Connect policies are described below:

- **CCM Android Policies**

  Dell Wyse Cloud Client Manager offers support for Android smartphone and tablet device management. All of these existing policies are also supported for management of Dell Wyse Cloud Connect devices. These options may be managed at all of the following levels: Default Policy Group; Group; Device; User.

  The policies supported are:

  - Passcode
  - Restrictions
  - Wi-Fi
  - PocketCloud RDP

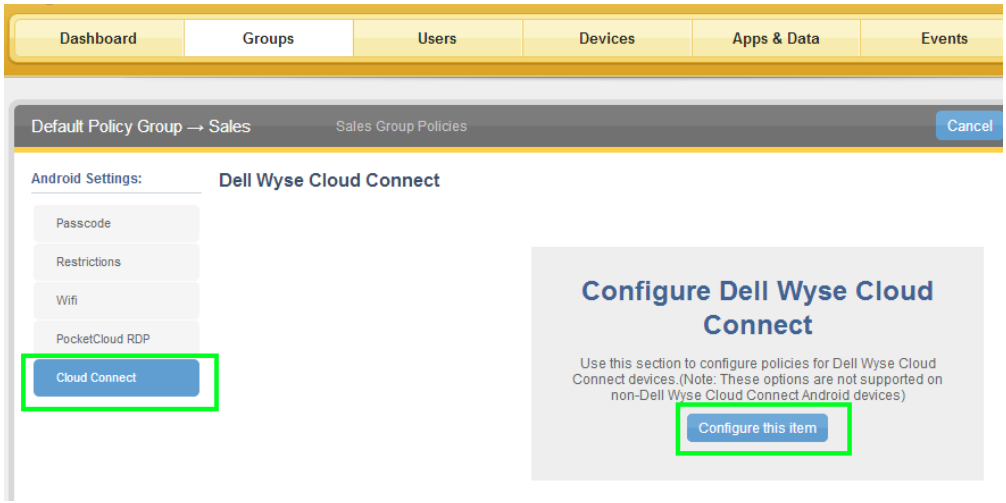

Dashboard
Groups
Users
Devices
Apps & Data
Default Policy Group
All users and devices are managed under this profile
Android Settings:
Passcode *
Restrictions
Wifi
PocketCloud RDP
Cloud Connect
Passcode
Required Passcode
Enforce the use of PIN, Password, or Pattern on the device
Require Alphabetic or Numeric
Require either a PIN or a Password on the device
Require Alphabetic
Require a Password with at least one alphabetic valued on the device
Require Alpha Numeric
Requires a Password with at least once alphabetic value and one numeric value on the device
Min Passcode Length
Smallest number of passcode characters allowed
5

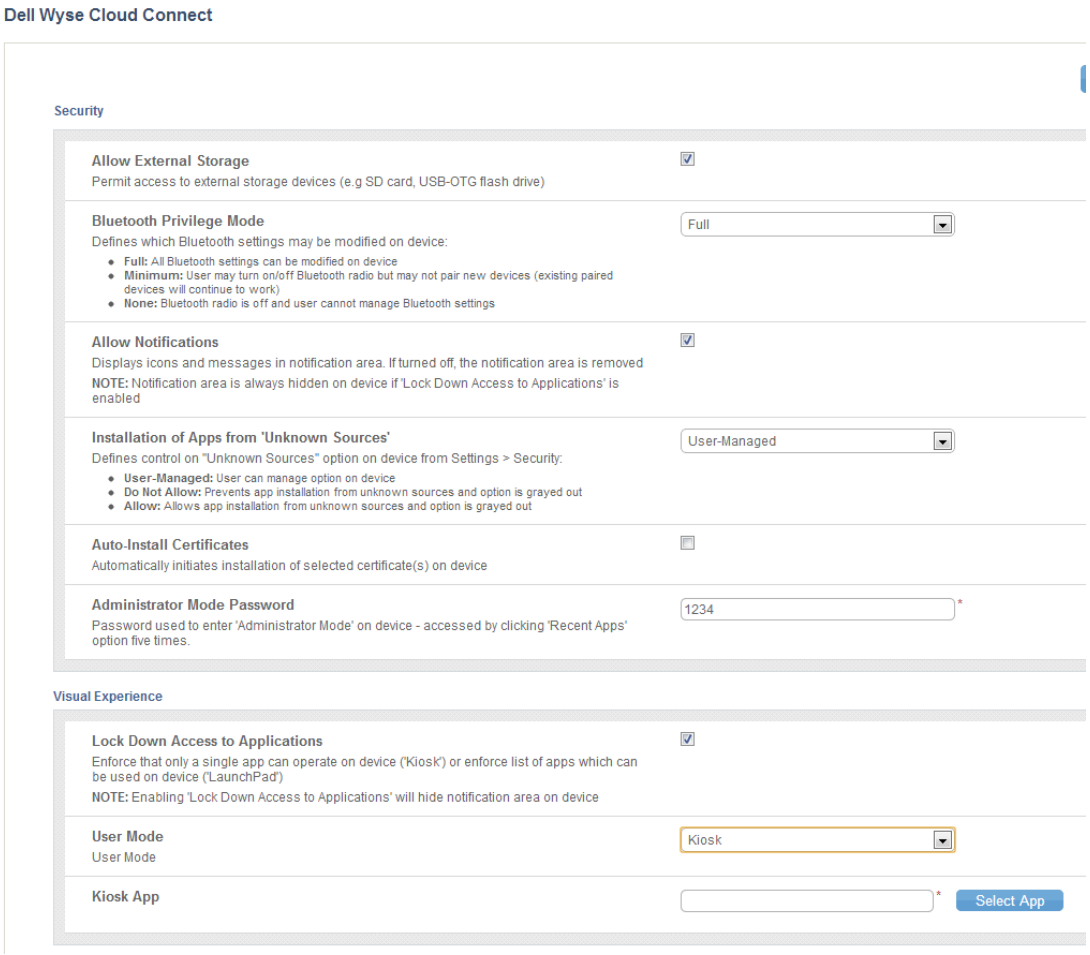
For further details on policy management hierarchy and Android device policies refer to the "**Cloud Client Manger - Administrators Guide**":
https://cloudclientmanagement.zendesk.com/entries/23891338

- **Dell Wyse Cloud Connect Policies** **[Requires Professional Tier]**

  New policies specific for Dell Wyse Cloud Connect devices are also available in addition to the Android device policies mentioned above. From the Android Settings there is new "**Cloud Connect**" tab from where these options may be managed.

  Click the "**Configure this item**" button to configure Dell Wyse Cloud Connect policies.




Dell Wyse Cloud Connect
Security
Allow External Storage
Permit access to external storage devices (e.g SD card, USB-OTG flash drive)
Bluetooth Privilege Mode
Defines which Bluetooth settings may be modified on device:
Full: All Bluetooth settings can be modified on device
Minimum: User may turn on/off Bluetooth radio but may not pair new devices (existing paired devices will continue to work)
None: Bluetooth radio is off and user cannot manage Bluetooth settings
Full
Allow Notifications
Displays icons and messages in notification area. If turned off, the notification area is removed
NOTE: Notification area is always hidden on device if 'Lock Down Access to Applications' is enabled
Installation of Apps from 'Unknown Sources'
Defines control on "Unknown Sources" option on device from Settings > Security:
User-Managed: User can manage option on device
Do Not Allow: Prevents app installation from unknown sources and option is grayed out
Allow: Allows app installation from unknown sources and option is grayed out
User-Managed
Auto-Install Certificates
Automatically initiates installation of selected certificate(s) on device
Administrator Mode Password
Password used to enter 'Administrator Mode' on device - accessed by clicking 'Recent Apps' option five times.
1234
Visual Experience
Lock Down Access to Applications
Enforce that only a single app can operate on device ('Kiosk') or enforce list of apps which can be used on device ('LaunchPad')
NOTE: Enabling 'Lock Down Access to Applications' will hide notification area on device
User Mode
User Mode
Kiosk
Kiosk App
Select App

The following policies are configurable from this page:

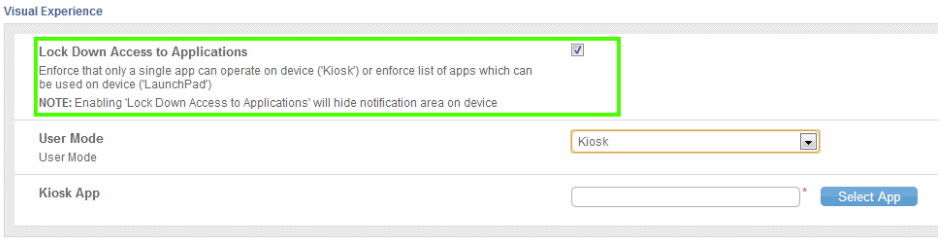
Allow External Storage	If unchecked, this option prevents access to external storage devices, such as SD cards, USB-OTG flash drives, etc.
Bluetooth Privilege Mode	Three management options for managing Bluetooth radio and pairing Bluetooth devices: 1. **Full**: User can turn on/off Bluetooth radio and pair new devices 2. **Minimum**: User may turn on/off Bluetooth radio. User may not add new paired devices. **Note**: Devices paired prior to policy being applied may continue to be used 3. **None**: Bluetooth radio is always off
Allow Notifications	If unchecked, notification area is removed from device. **NOTE**: When "Lock Down Access to Applications" option is enabled, this setting is disregarded and the notification area is always removed.
Installation of Apps from 'Unknown Sources'	This manages the device option from **Settings > Security > "Unknown Sources"**. "**Unknown Sources**" option must be checked to allow installation of apps from outside of Google Play Store. When option is unchecked, user will not be able to manually install apps outside of Google Play Store. Three options are supported: 1. **User-Managed**: User can turn on/off option 2. **Do Not Allow:** Option is unchecked and setting cannot be modified by user on device 3. **Allow:** Option is checked and setting cannot be modified by user on device **NOTE**: Cloud Client Manager supports installation of Enterprise Apps for all Android devices. If these apps are configured as "Mandatory" by policy (from **Apps & Data > Application > Policies**), these apps will still be silently installed on device even if "**Unknown Sources**" option is unchecked on device.
Auto-Install Certificates	Selecting this option will load list of **Certificates** uploaded to the **File Repository Inventory** page (from ***Apps & Data > File Repository > Inventory***). **Certificates**: Select the certificates to be auto-installed on Dell Wyse Cloud Connect devices. **NOTE**: This option is only for automating the deployment of certificates. Deselecting certificates from the policy will not remove any certificate already installed on the device. Refer to "**Cloud Client Manger - Administrators Guide**" for details on adding certificates: https://cloudclientmanagement.zendesk.com/entries/23891338
Administrator Mode Password	This is a configurable password for devices that are operating in **Kiosk** or **LaunchPad** modes (see below for details) in order to temporarily access other device settings. When device is operating in either **Kiosk** or **LaunchPad** mode, click the "Recent Apps" button 5 times quickly (within 2 seconds) and enter this password when prompted. For device to reapply previous policies and exit Administrator Mode, either select the "Reapply Policies" option from CCM Agent or republish policies to device from CCM Server.

Lock Down Access to Applications	Use this option to lock down device to either a single application or a list of applications. Selecting this option will enable selection of one of the following **User Modes**: 1. **Kiosk Mode**: Limits the device to only operating a single app. In this mode the Home button, Recent Apps button, and Notification Area disabled on device. 2. **LaunchPad Mode**: Limits the device to only allowing user to run one of the configured apps from the LaunchPad Apps list. In this mode the Home button return user to a screen where they can select from the list of configured LaunchPad Apps. The Notification Area is removed from the device. **NOTE**: A maximum of eight LaunchPad Apps are configurable. Refer to "**Configuring Kiosk and LaunchPad Modes"** section below for more details on configuring Kiosk and LaunchPad modes. **NOTE**: Enabling 'Lock Down Access to Applications' will hide notification area on device regardless of setting of **"Allow Notifications"** option above.

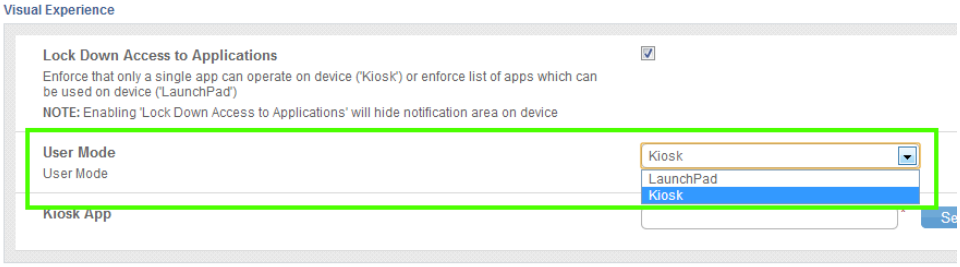
- **Configuring Kiosk and LaunchPad Modes** **[Requires Professional Tier]**

  To lock down the device to either a single application (**Kiosk Mode**) or a defined list of applications (**LaunchPad Mode**), follow the instructions below:

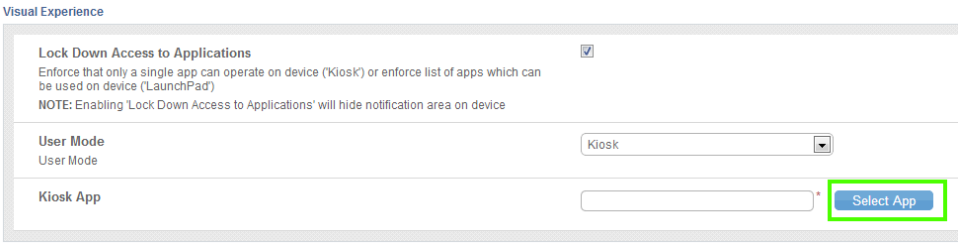
  i. Check the "**Lock Down Access to Applications**" checkbox


Visual Experience
Lock Down Access to Applications
Enforce that only a single app can operate on device ('Kiosk') or enforce list of apps which can be used on device ('LaunchPad')
NOTE: Enabling 'Lock Down Access to Applications' will hide notification area on device
User Mode
User Mode
Kiosk
Kiosk App
Select App

  ii. Select the **User Mode** (Kiosk or LaunchPad)


Visual Experience
Lock Down Access to Applications
Enforce that only a single app can operate on device ('Kiosk') or enforce list of apps which can be used on device ('LaunchPad')
NOTE: Enabling 'Lock Down Access to Applications' will hide notification area on device
User Mode
User Mode
Kiosk
LaunchPad
Kiosk
Kiosk App

iii. For **Kiosk Mode**, click the "**Select App**" button

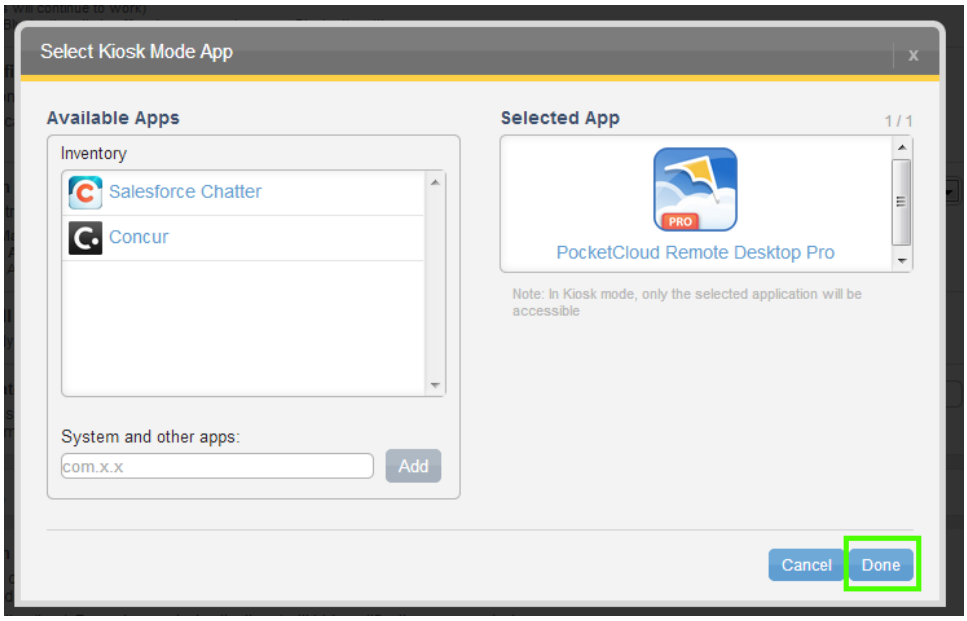

Visual Experience
Lock Down Access to Applications
Enforce that only a single app can operate on device ('Kiosk') or enforce list of apps which can be used on device ('LaunchPad')
NOTE: Enabling 'Lock Down Access to Applications' will hide notification area on device
User Mode
User Mode
Kiosk
Kiosk App
Select App

In the "**Select Kiosk Mode App**" window, double-click one of the apps from the "**Available Apps**" list on the left-side.

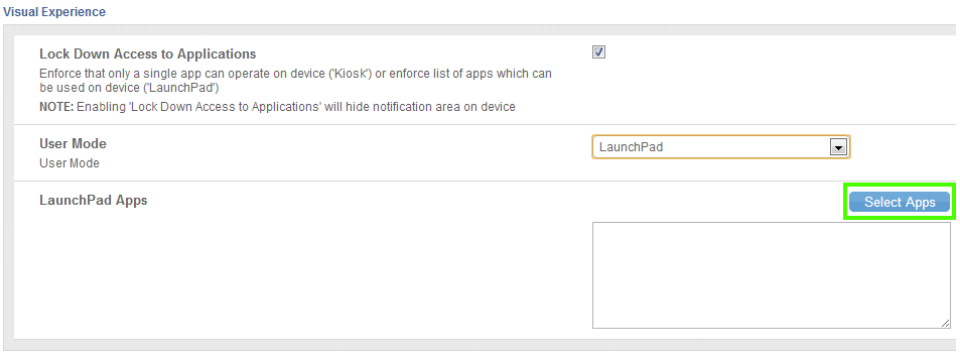
The "**Available Apps**" list is composed of Android apps added to the Application Inventory (from ***Apps & Data > Applications > Inventory***).

Alternately, for apps that do not appear in this list the Application Identifier for the desired app (typically of format "com.x.x.") can manually be configured using the textbox at bottom of panel – click **Add** to add the app to the **Selected Apps** box.

Once the desired application appears in the **Selected App** box, click "**Done**".



iv. For **LaunchPad Mode**, click the "**Select Apps**" button

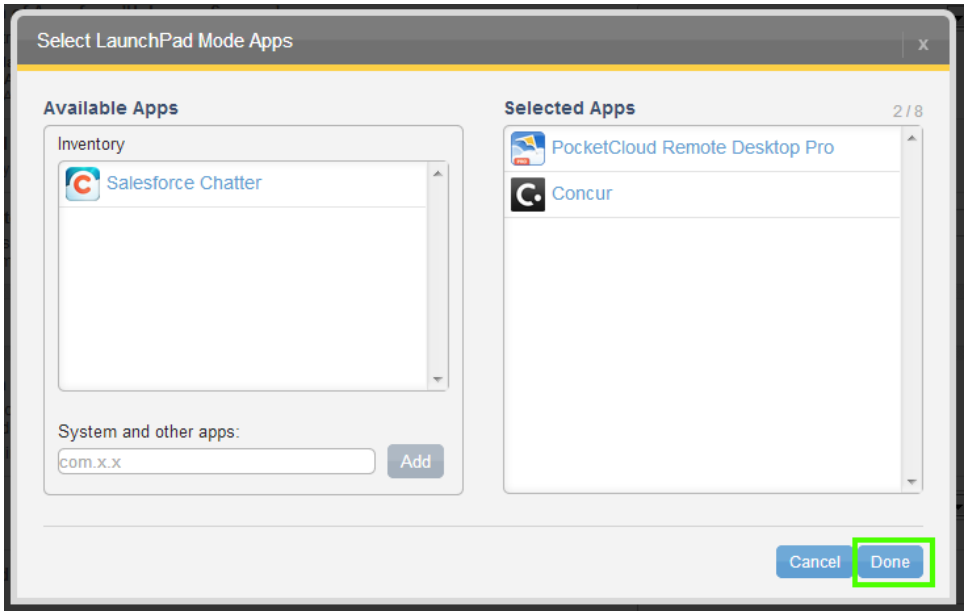

Visual Experience
Lock Down Access to Applications
Enforce that only a single app can operate on device ('Kiosk') or enforce list of apps which can be used on device ('LaunchPad')
NOTE: Enabling 'Lock Down Access to Applications' will hide notification area on device
User Mode
User Mode
LaunchPad
LaunchPad Apps
Select Apps

In the "**Select LaunchPad Mode Apps**" window, double-click any of the apps from the "**Available Apps**" list on the left-side. Up to eight apps can be added to the "**Selected Apps**" list.

The "**Available Apps**" list is composed of Android apps added to the Application Inventory (from ***Apps & Data > Applications > Inventory***).

Alternately, for apps that do not appear in this list the Application Identifier for the desired app (typically of format "com.x.x.") can manually be configured using the textbox at bottom of panel – click **Add** to add the app to the "**Selected Apps**" list.

Once all the apps have been added to the **Selected Apps** list, click "**Done**".

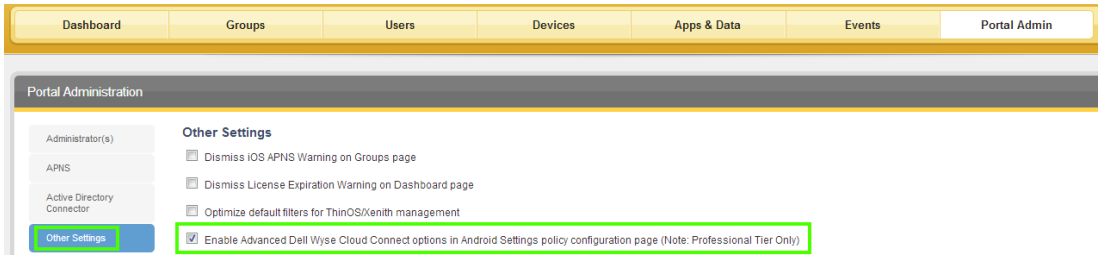


- **<u>Configuring Advanced Options</u>** **[Requires Professional Tier]**

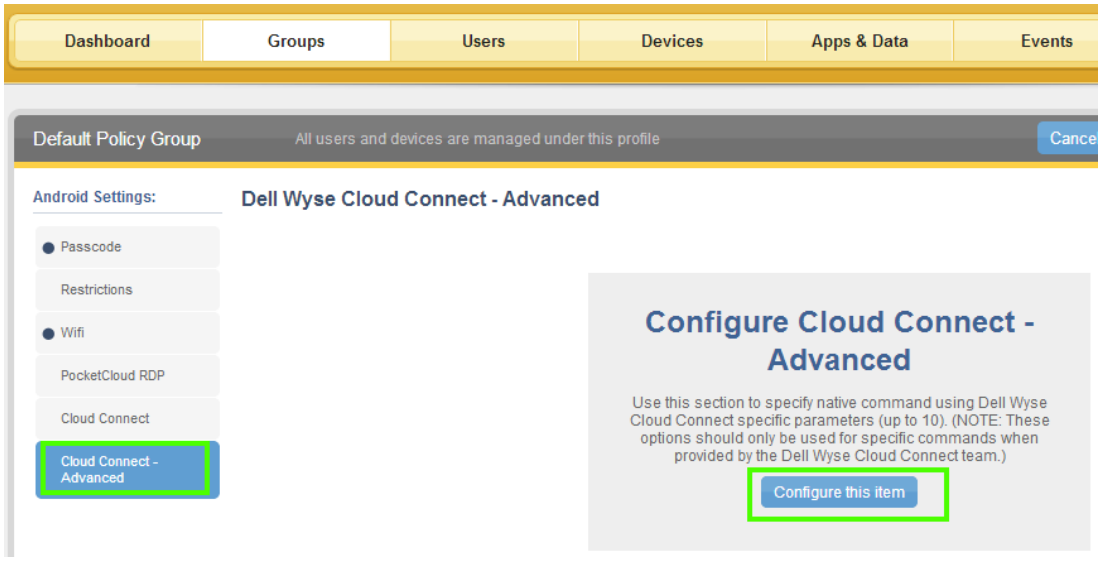
  Dell Wyse Cloud Connect supports the configuration of additional options for specific advanced scenarios using native device commands.

  NOTE: This options are recommended to only be used when provided by Dell Wyse Cloud Connect team.

  To enable configuration of advanced options, from **Portal Admin > Other Settings**, check the option for: "***Enable Advanced Dell Wyse Cloud Connect options in Android Settings policy configuration page (Note: Professional Tier Only)***"



Once the option above is configured, from the **Android Settings** policy page there will now be an additional tab at the bottom called "**Cloud Connect – Advanced**". From this tab click the "**Configure this item**" button to configure the advanced commands provided to you.

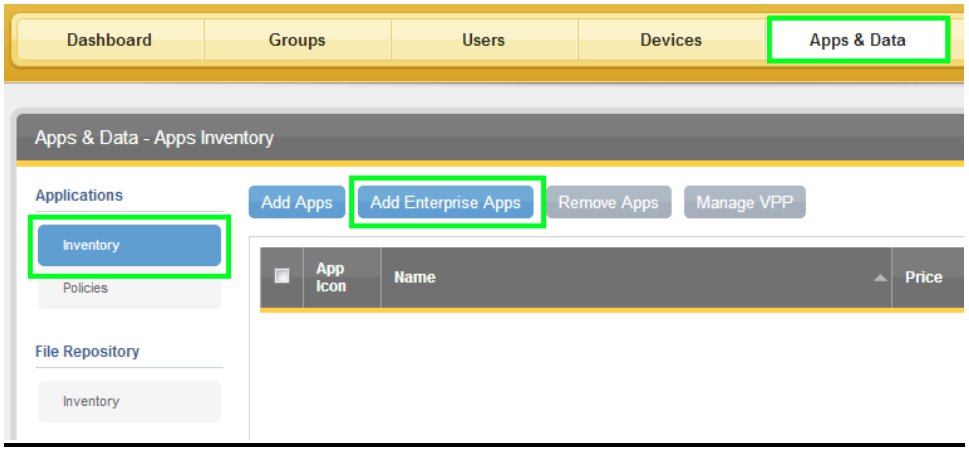

Dashboard
Groups
Users
Devices
Apps & Data
Events
Default Policy Group
All users and devices are managed under this profile
Cance
Android Settings:
Dell Wyse Cloud Connect - Advanced
Passcode
Restrictions
Wifi
PocketCloud RDP
Cloud Connect
Cloud Connect - Advanced
Configure Cloud Connect - Advanced
Use this section to specify native command using Dell Wyse Cloud Connect specific parameters (up to 10). (NOTE: These options should only be used for specific commands when provided by the Dell Wyse Cloud Connect team.)
Configure this item

2. Enterprise App Store

In-house developed apps may now be managed via the Cloud Client Manager console. This allows custom iOS and Android apps to be added to the Application Inventory and have policies applied to them.

To add application to Enterprise App Store:

a) From **Apps & Data > Inventory**, click the "**Add Enterprise Apps**" button



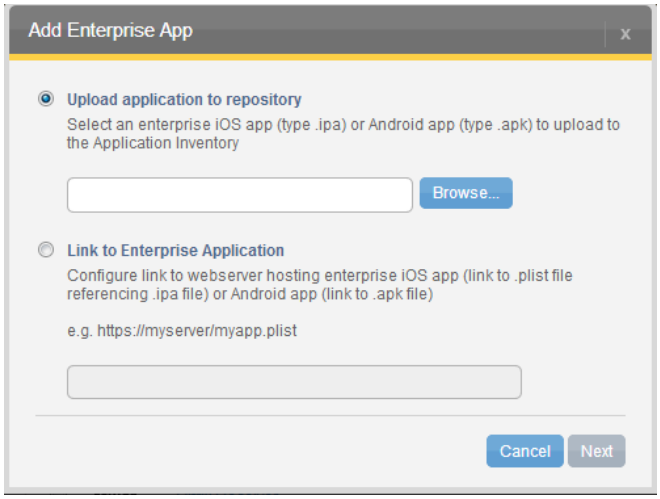
b) Select to either upload the app to the CCM repository (*Upload application to repository*) or to provide a link to a webserver where the application is hosted (*Link to Enterprise Application*).

If app is uploaded to CCM repository:

- iOS apps: select the app file (type .ipa)
- Android apps: select the app file (type .apk)

If a link is being provided to app:

- iOS apps: provide the URL to the .plist file which references the .ipa file (consult Apple developer documentation on how to prepare apps for wireless distribution)
- Android apps: select the app file (type .apk)

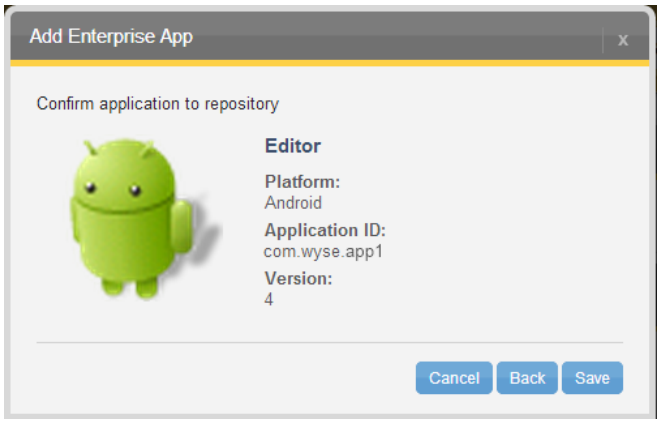

Add Enterprise App
x
Upload application to repository
Select an enterprise iOS app (type .ipa) or Android app (type .apk) to upload to the Application Inventory
Browse...
Link to Enterprise Application
Configure link to webserver hosting enterprise iOS app (link to .plist file referencing .ipa file) or Android app (link to .apk file)
e.g. https://myserver/myapp.plist
Cancel
Next

NOTE: if using the *Link to Enterprise Application* option the app should be stored on a secured server (https).

Once the method is configured and app selected, click "**Next**".

c) If uploading application to the inventory, review the information on screen and click "**Save**" to add the app to the Application Inventory. For iOS you can optionally add an icon to display in the CCM console).

If providing a link to the enterprise application, configure the requested app info (App Name; App ID; Version and option to upload an icon to display in CCM console). For iOS, you will also need to provide the device types that the app supports (iPhone & iPad, iPhone only, or iPad only). **NOTE**: If the incorrect App ID is provided the app will not be manageable from the CCM console.

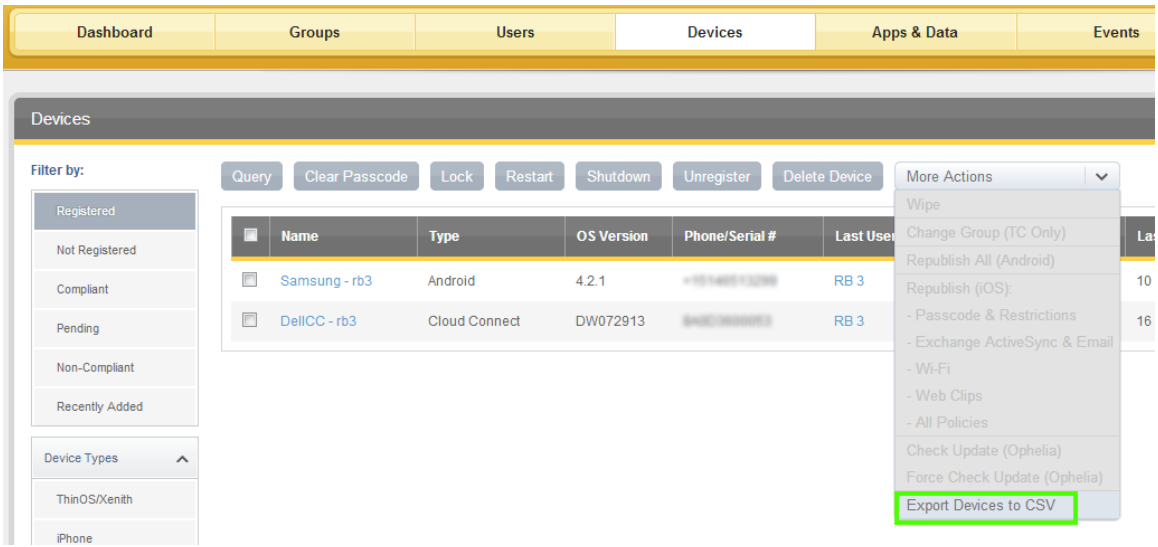


3. Device Inventory Exportable Report

The asset information for Cloud Client Manger managed devices can now be exported to a CSV file from the portal.

From the **Devices** page, select ***More Actions > Export Devices to CSV*** option.

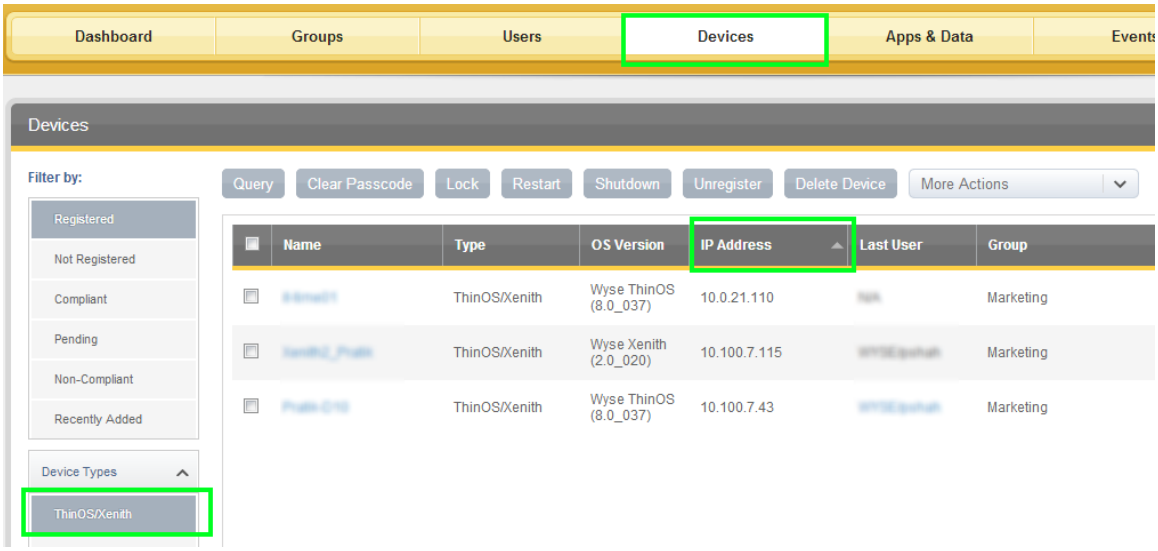
This will automatically generate a CSV with a list of the asset information for all the devices currently filtered on screen.



4. Sort by IP Address

From the **Devices** page, ThinOS and Xenith devices are now sortable by IP Address.

To sort by IP Address, ensure that "**ThinOS/Xenith**" is selected from **Device Types** filter and then click the "**IP Address**" column header in the devices table.



- ## Supported Devices

Thin Client Requirements

- **Supported Devices:** Thin Clients supported include:
  - C00X (Wyse Xenith) running firmware 2.0_021 or later (**recommended 2.0_026 or later)**
  - R00LX (Wyse Xenith Pro) running firmware 2.0_021 or later (**recommended 2.0_026 or later)**
  - T00X (Xenith 2) running firmware 2.0_021 or later **(recommended 2.0_026 or later)**
  - C10LE running firmware ThinOS 7.1_207 or later (**recommended 8.0_037 or later)**
  - R10L running firmware ThinOS 7.1_207 or later (**recommended 8.0_037 or later)**
  - T10 running firmware ThinOS 7.1_207 or later (**recommended 8.0_037 or later)**
  - D10D running firmware ThinOS 7.1_207 or later (**recommended 8.0_037 or later)**

  For supported thin clients running earlier versions, a firmware update is required to enable Cloud Client Manager connectivity. Updates can be downloaded from the Wyse Self-Service Center at: http://support.wyse.com/selfservice.html

  IMPORTANT: You must use your *ThinOS Maintenance* (you should have received an email from Wyse or your reseller with full instructions) to obtain available firmware updates (if you did not receive this email, contact your reseller). If unfamiliar with updating firmware on Wyse ThinOS cloud clients, refer to Wyse Knowledge Base Solution #**10566** (go to Wyse Knowledge Base at http://www.wyse.com/kb and search for **10566**).
- **Connectivity Requirements:**
  - TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com

Dell Wyse Cloud Connect Requirements

- **Connectivity Requirements:**
  - TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com

iOS Requirements

- **Supported Devices:**
  - iPhone and iPad running iOS Version 5.x and later
- **Connectivity Requirements:**
  - TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 80 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 8443 (outbound) to us1-mdm.cloudclientmanager.com
  - TCP port 5223 (outbound) - for Apple APNS
- **MDM Certificate Requirements:**
  - A Mobile Device Management (MDM) Apple Push Notification Service (APNs) certificate is required for iOS device management - this requires an Apple ID. As the Apple ID account will be linked to the APNs certificate, which must be renewed annually, a corporate Apple ID account should be used and not a personal one

Android Requirements

- **Supported Devices:**
  - Devices running Android Version 2.3 and later
- **Connectivity Requirements:**
  - TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com

"R2" Release (June 28, 2013)

- **Release Overview**

This release focuses on enhancing thin client management by enabling cloud-based firmware upgrades and certificate deployment for ThinOS-based thin clients. Firmware and certificate management is efficient and flexible - updates can be made globally, or targeted to specific policy groups or even specific devices.

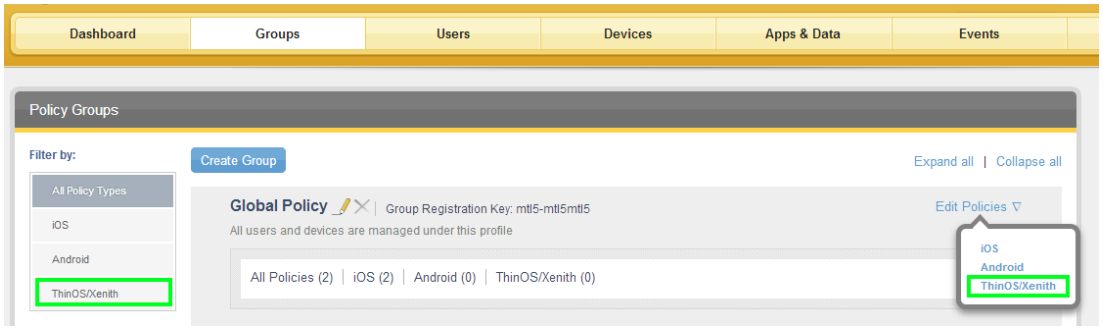
Highlights of this release:

- **Thin client file repository**
  - Simplified management for ThinOS-based thin client firmware and certificates
  - Enhanced visibility into file information: version, platform, description, etc.
- **Policy-based deployment of firmware**
  - Assign firmware at global, group or per-device level for ThinOS-based thin clients **NOTE**: Remote firmware imaging from cloud is supported with ThinOS firmware version 8.0_037 or later
  - Smart detection of cloud-based vs local imaging
- **New platform support**
  - D10D (ThinOS) thin client platform
  - iPod Touch devices
- **Other Enhancements**
  - Messaging for 'queued' jobs
  - Optimizations for automated deployments (i.e DHCP/INI-based registrations)

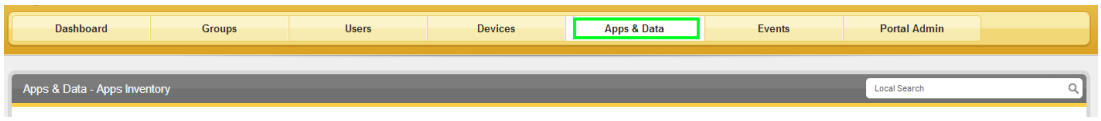
- **New Features Details**

1. UI Changes & Optimizations

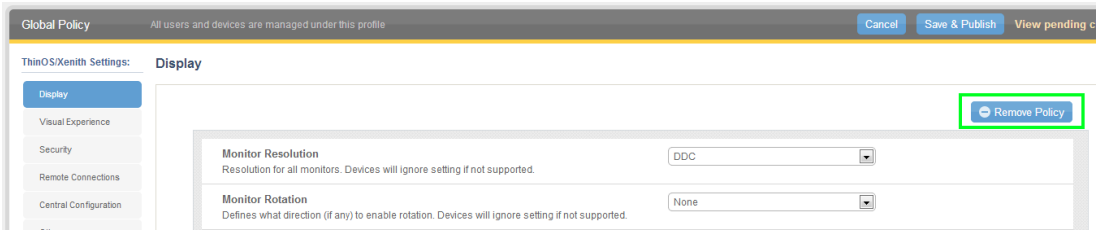
a) "**Thin Client**" policy references renamed to "**ThinOS/Xenith**" in **Groups** page



b) "**Apps**" tab renamed to "**Apps & Data**"

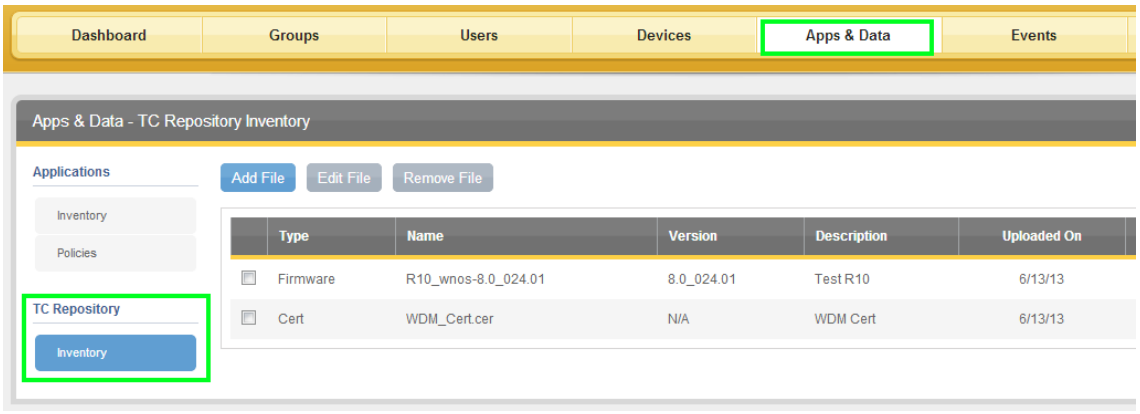


c) Easier to locate the "**Remove Policy**" button



2. Thin client repository

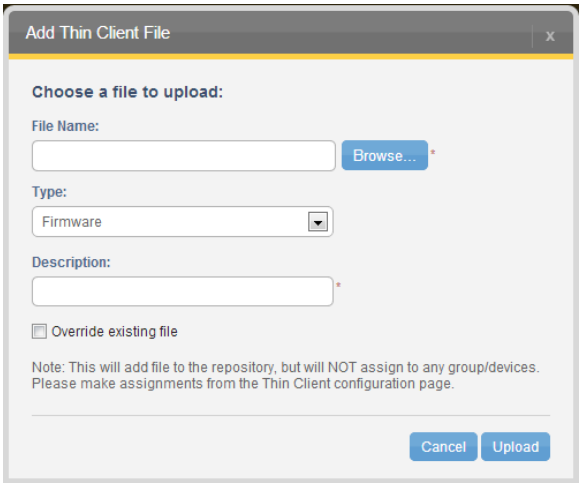
New thin client firmware repository: From "**Apps & Data** tab **> TC Repository > Inventory"**, options to manage firmware image and certificate files.



a) Adding files to inventory:

i. Click "**Add File**" from the **TC Repository Inventory** page.

ii. Browse to a firmware or certificate file, select "**Type**" (Firmware or Certificate) and provide a description.



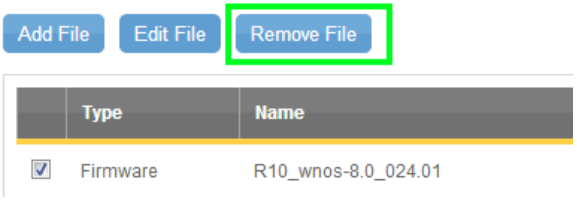
Optionally, select to "**Override existing file**".

iii. File will be added to inventory.

NOTE: For ThinOS firmware images, the file version and platform will be auto-detected

b) Editing files in inventory: Select an existing file and click "**Edit File**" button to update the description assigned to a firmware or certificate file.

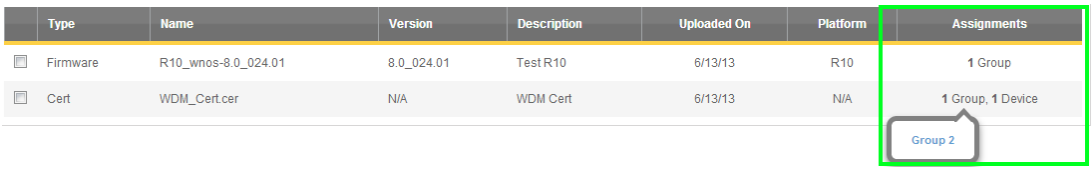
c) Removing files from inventory: Select an existing file and click "**Remove File**" button to remove file from inventory.



NOTE: Files assigned to a policy group or a device cannot be removed from inventory ("**Remove File**" button will be disabled)

d) Assigning files: Files are assigned to policy groups or to devices from either the Groups page (ThinOS/Xenith) or from the Device Details page by assigning an exception at device level. See **Error! Reference source not found.** section below for details. The policy assignments an be reviewed from the **TC Repository Inventory** page.

The number of policy groups and devices (device-level exceptions) that each file has been assigned to is displayed in the assignments column. By hovering over the number next to "Groups" or "Devices" it will display the names of the policy groups and devices.

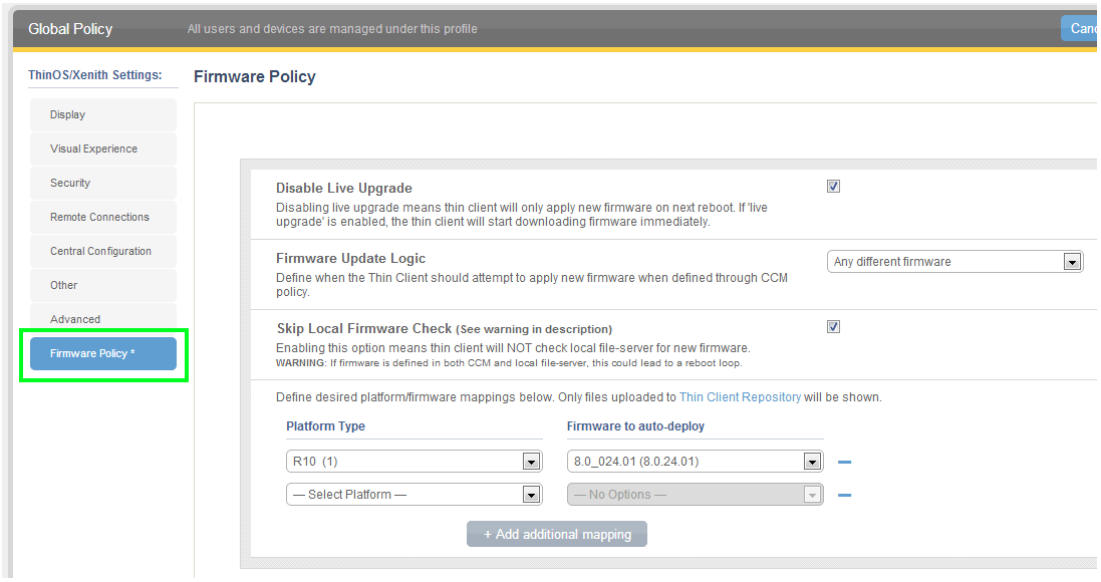


3. Policy-based firmware deployment

a) New **Firmware Policy** tab: assign policies for firmware images uploaded to **TC Repository Inventory** page.

Firmware policies can be managed at Global level, group level or device level.

NOTE: Remote firmware imaging from cloud is supported with firmware version 8.0_037 or later


Global Policy
All users and devices are managed under this profile
ThinOS/Xenith Settings:
Firmware Policy
Display
Visual Experience
Security
Remote Connections
Central Configuration
Other
Advanced
Firmware Policy *
Disable Live Upgrade
Disabling live upgrade means thin client will only apply new firmware on next reboot. If 'live upgrade' is enabled, the thin client will start downloading firmware immediately.
Firmware Update Logic
Define when the Thin Client should attempt to apply new firmware when defined through CCM policy.
Any different firmware
Skip Local Firmware Check (See warning in description)
Enabling this option means thin client will NOT check local file-server for new firmware.
WARNING: If firmware is defined in both CCM and local file-server, this could lead to a reboot loop.
Define desired platform/firmware mappings below. Only files uploaded to Thin Client Repository will be shown.
Platform Type
Firmware to auto-deploy
R10 (1)
8.0_024.01 (8.0.24.01)
— Select Platform —
— No Options —
+ Add additional mapping

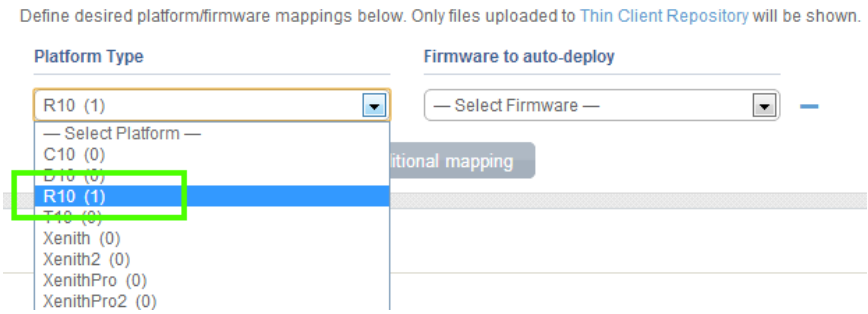
- **Disable Live Upgrade**: "Live Upgrade" means the thin client will immediately begin downloading and apply new firmware based on defined policies. If you prefer that the thin client only check for new firmware on each bootup, then you can disable "Live Upgrade".
- **Firmware Update Logic**: This option determines how the thin client behaves when a new firmware is published from Cloud Client Manager. The options are:
  i. *Any different firmware*: Thin client will update firmware to version assigned by Cloud Client Manager policy (even if version is lower than current image on device)
  ii. *New firmware only*: Thin client updates firmware only when a newer version is assigned to Cloud Client Manager policy
  iii. *Do not update*: Thin client ignores firmware versions assigned to Cloud Client Manager policies
- **Skip Local Firmware Check**: When enabled, thin client will bypass local fileserver checks for firmware updates.

  NOTE: It is HIGHLY recommended to always have this option enabled if you define firmware on CCM. Otherwise, if you have firmware policies in CCM and firmware located on local file server, it will lead to an endless reboot as the thin client applies differing images. This option is available to assist in certain migration scenarios where this flexibility is needed.

- **Platform Type / Firmware version assignment**: This section maps specific firmware versions to different platform types (e.g. T10, R10, Xenith Pro, etc.) allowing for different firmware versions to be assigned to different platforms.

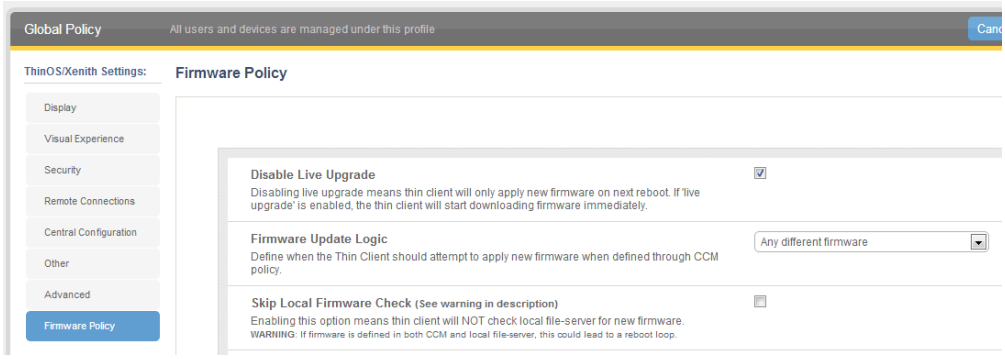
  To map a platform type a specific firmware version select the desired platform from the "**Platform Type**" dropdown selection list and then select the desired firmware version from the "**Firmware to auto-deploy**" dropdown list. The list of platform types displays in parentheses the number of firmware versions currently uploaded to the **TC Repository Inventory** page that are supported.

  For example, in the screen capture below there is one firmware version available from the **TC Repository Inventory** page that can be mapped to R10 thin clients.



b) Updates to options:

- **Firmware Update Logic**: moved from the **Central Configuration** tab to the **Firmware Policy** tab.
- **Local Prompt**: Removed from the **Central Configuration** tab; updated with "**Disable Live Upgrade** option in the **Firmware Policy** tab.

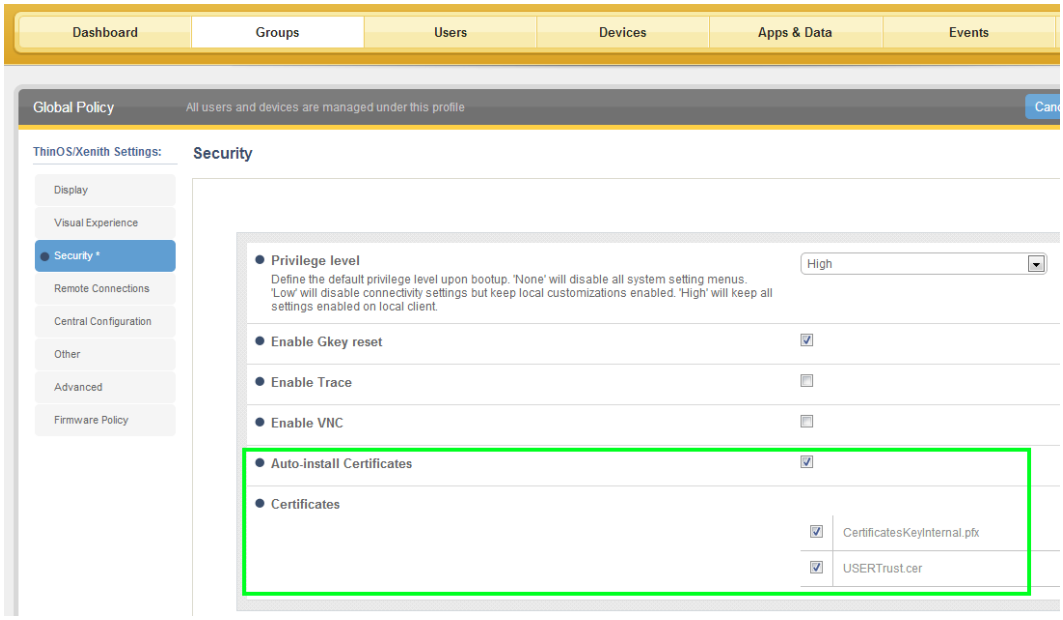

Global Policy
All users and devices are managed under this profile
ThinOS/Xenith Settings:
Firmware Policy
Display
Visual Experience
Security
Remote Connections
Central Configuration
Other
Advanced
Firmware Policy
Disable Live Upgrade
Disabling live upgrade means thin client will only apply new firmware on next reboot. If 'live upgrade' is enabled, the thin client will start downloading firmware immediately.
Firmware Update Logic
Define when the Thin Client should attempt to apply new firmware when defined through CCM policy.
Any different firmware
Skip Local Firmware Check (See warning in description)
Enabling this option means thin client will NOT check local file-server for new firmware.
WARNING: If firmware is defined in both CCM and local file-server, this could lead to a reboot loop.

4. Policy-based certificate deployment

a) New options added to **Security** tab to assign policies for certificates uploaded to **TC Repository Inventory** page.

NOTE: Remote firmware imaging from cloud is supported with ThinOS firmware version 8.0_037 or later

Certificate assignment can be managed at Global level, group level or device level.



- **Auto-Install Certificates**: Selecting this option will load list of **Certificates** uploaded to the **TC Repository Inventory** page.
- **Certificates**: Select the certificates to be auto-installed on thin clients.

  NOTE: This option is only for automating the deployment of certificates. Unselecting from policy will not remove any certificate already installed on the device.

5. Group Registration Key Enhancements

a) **Group Registration Key** for thin client device registration can be applied from multiple sources. They will be read in the following order and the last one detected takes precedence:

i. DHCP Option Tag 199
ii. INI configuration file (*e.g.* ***ccmenable=yes groupkey=abc1…***)
iii. Local configuration on thin client (from ***Central Configuration > CCM*** *tab*)
OR
Receive **Group Registration Key** update from Cloud Client Manager as part of a "**Change Group**" request.

b) The **Group Registration Key** assigned by DHCP option tag 199 or from an INI configuration file are primarily used for first-time registration - see item Error! Reference source not found. elow for exception case. These settings are only applied if either of following conditions are met:

i. Option "**Enable Cloud Client Manager (CCM)**" is disabled from ***Central Configuration > CCM*** *tab*
ii. Option "**Enable Cloud Client Manager (CCM)**" is enabled from ***Central Configuration > CCM*** *tab*, however the **Group Registration Key** is not configured.

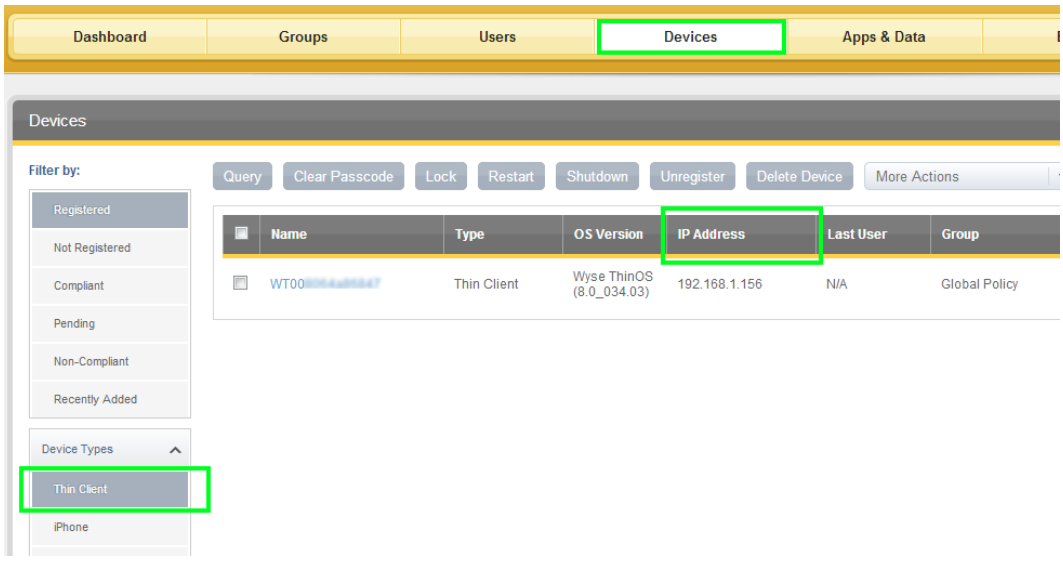
NOTE: If a **Group Registration Key** is defined using DCHP option tag 199 or from INI configuration file command and the thin client is already registered, there will be a message

in the thin client **Event Log** notifying that the centrally defined **Group Registration Key** is being ignored.

c) A new INI option "**override=yes**" can be added to the "**ccmenable=**" INI parameter which will always apply even if thin client already has CCM enabled. In this case the INI configuration file can enforce that the thin client uses the configured **Group Registration Key** from INI file during device boot even when the device was already registered with Cloud Client Manager.

6. Other Enhancements

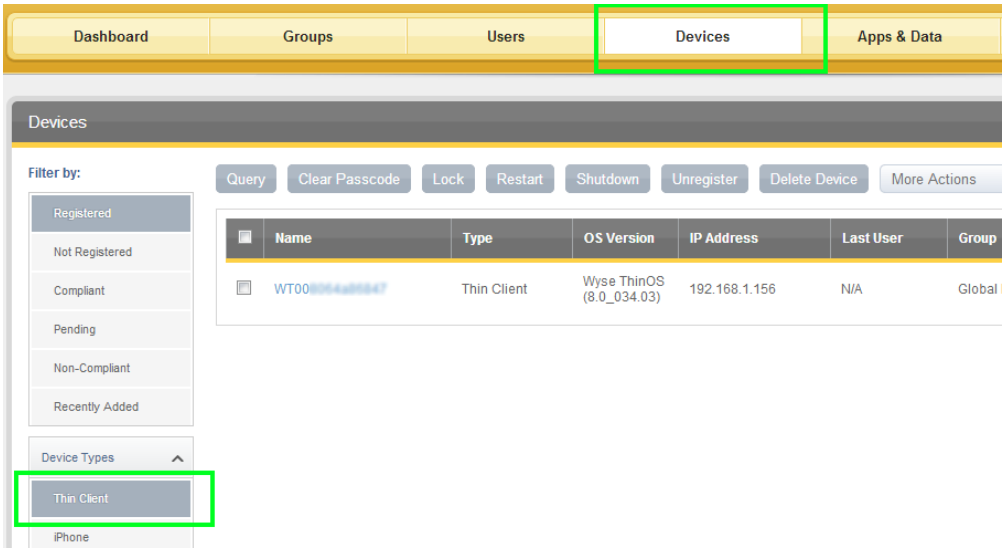
a) In **Devices** page, when selecting the "**Thin Client**" filter the column "**Phone/Serial #**" is replaced by "**IP Address**".



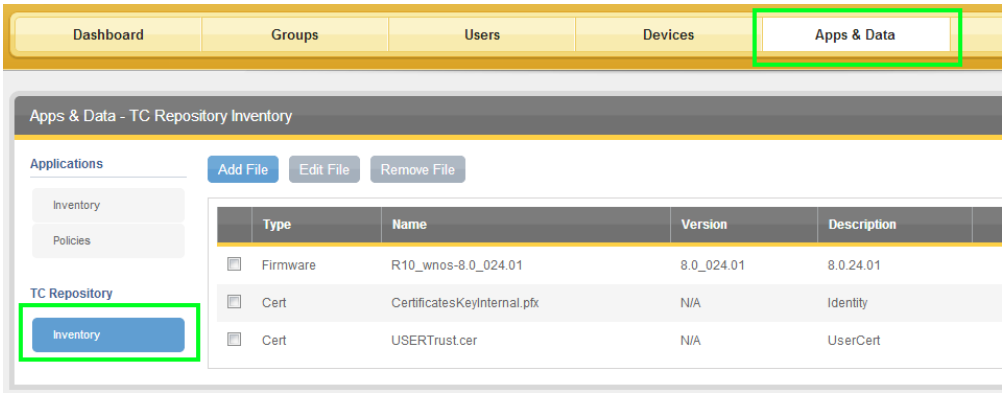
b) New option in **Portal Admin > Other Settings** tab: ***Optimize default filters for Thin Client management***

When this option is enabled, the default views for following pages will be optimized for thin client management:

i. In **Devices** page, the "**Thin Client**" filter is selected by default



ii. In **Apps & Data** page, the "**TC Repository Inventory**" page is loaded by default.



- ## Supported Devices

Thin Client Requirements

- **Supported Devices:** Thin Clients supported include:
  - C00X (Wyse Xenith) running firmware 2.0_021 or later (**recommended 2.0_026 or later)**
  - R00LX (Wyse Xenith Pro) running firmware 2.0_021 or later (**recommended 2.0_026 or later)**
  - T00X (Xenith 2) running firmware 2.0_021 or later **(recommended 2.0_026 or later)**
  - C10LE running firmware ThinOS 7.1_207 or later (**recommended 8.0_037 or later)**
  - R10L running firmware ThinOS 7.1_207 or later (**recommended 8.0_037 or later)**
  - T10 running firmware ThinOS 7.1_207 or later (**recommended 8.0_037 or later)**
  - D10D running firmware ThinOS 7.1_207 or later (**recommended 8.0_037 or later)**

  For supported thin clients running earlier versions, a firmware update is required to enable Cloud Client Manager connectivity. Updates can be downloaded from the Wyse Self-Service Center at: http://support.wyse.com/selfservice.html

  IMPORTANT: You must use your *ThinOS Maintenance* (you should have received an email from Wyse or your reseller with full instructions) to obtain available firmware updates (if you did not receive this email, contact your reseller). If unfamiliar with updating firmware on Wyse ThinOS cloud clients, refer to Wyse Knowledge Base Solution #**10566** (go to Wyse Knowledge Base at http://www.wyse.com/kb and search for **10566**).

- **Connectivity Requirements:**
  - TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com

iOS Requirements

- **Supported Devices:**
  - iPhone, iPad, iPod Touch devices running iOS Version 5.x and later

- **Connectivity Requirements:**
  - TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 80 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 8443 (outbound) to us1-mdm.cloudclientmanager.com
  - TCP port 5223 (outbound) - for Apple APNS

- **MDM Certificate Requirements:**
  - A Mobile Device Management (MDM) Apple Push Notification Service (APNs) certificate is required for iOS device management - this requires an Apple ID. As the Apple ID account will be linked to the APNs certificate, which must be renewed annually, a corporate Apple ID account should be used and not a personal one

Android Requirements

- **Supported Devices:**
  i. Devices running Android Version 2.3 and later

- **Connectivity Requirements:**
  i. TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  ii. TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com

Known Issues

STR-678	iOS registration fails if re-registering within 30 seconds
STR-842	Some iOS/Android sub-options at lower policy level not affected by changes to parent options at higher policy level
STR-1148	Android device prompts for app install for installed System apps
STR-1173	Remove certificate for iOS payload fails unless linked payload is removed
STR-1409	Picture taken from the Android back camera compressed on Agent display (correct on server)
STR-1497	iOS Webclip uploaded image truncated in IE8 in CCM console
STR-2335	User/Device Details summary view not displaying some iOS settings when payload configured at higher level is saved with default settings at user/device level.
STR-2356	Formatting issues in app policy UI for policy groups with long group names
STR-2414	Event missing when removing device-level exception payloads
STR-2449	Cannot deactivate AD user missing required user information
STR-2489	Apps installed from App Store not tagged as “not managed” in CCM Agent when user cancels the app install request on device
STR-2552	VPP file name is not cleared if upload is cancelled and reinitiated
STR-2613	Feedback missing on iOS Agent when trying to initiate paid app install and no redemption code available
STR-2675	Some Thin Client CCM policies override policies set in Global .ini
STR-2712	Some Android devices displaying app identifier instead of app name in Restrictions message
STR-2726	Extra remove profile command generated when assigning two payloads for same policy type at different policy levels
STR-2729	During Thin Client registration, in specific scenario device shows as compliant even if configuration could not be loaded.
STR-2786	Changing Android app policy multiple times between mandatory to not managed may cause extra remove application commands
STR-2922	Changing Android policy sometimes requires Republish to push policies
CCMPC-137	Passcode policy not removed from device when restriction applied at lower level and passcode applied/removed at default policy group level
STR-3009	In Thin Client system information, the “802.1X Auth” field may report N/A when invalid characters received
STR-3105	In Dashboard, Devices, User Details, User Invitations, Portal Admin views labels are not updated (“Thin Client” to “ThinOS/Xenith”) for R2 release
STR-3107	If Thin Client firmware policy “Skip local firmware check” is unchecked and different firmware versions are available from CCM and local file server, device will reboot continuously
STR-3108	Thin Client firmware policy “Skip local firmware check” is ignored if no firmware mappings are configured in CCM policy
STR-3109	Thin Client will not revert Global Thin Client firmware mapping in case where a device-level exception has been pushed to device and reverted by using “Select Firmware” option. Workaround: Remove policy from device level exception

- **Issues resolved in this release**

STR-3030	Application missing from Installed Apps list for iOS and Android applications with same bundle/application identifier
STR-3031	Registered thin client does not go to “Pending” status after group change (delete group action)
STR-3033	Layout issues with IE “Compatibility View” feature enabled
STR-3112	Cannot create accounts with “-“ character in the domain field of Email Address

"R1" Release (May 24, 2013)

- **Release Overview**

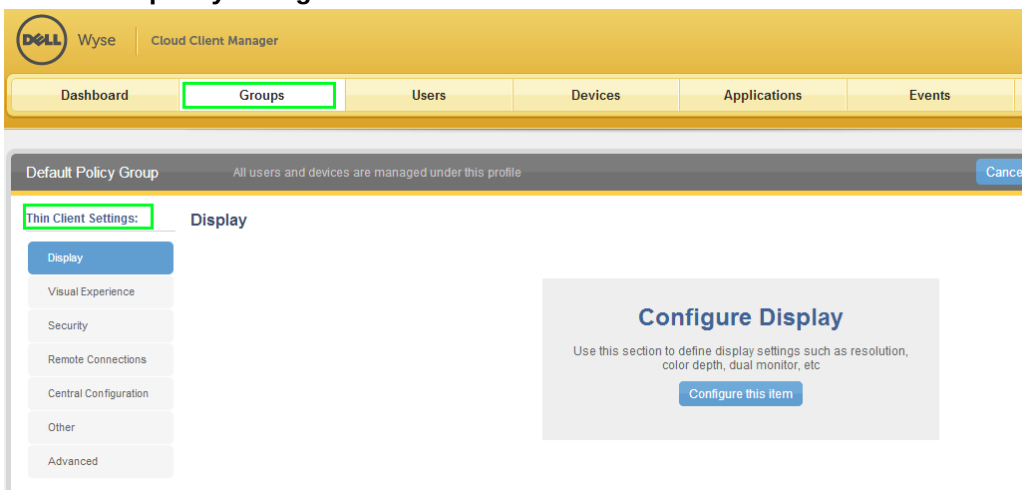
  Some of the highlights of this release:

  - Support for new Thin Client management policies
  - Active Directory integration for CCM mobile user management
  - Support for the Apple VPP program
  - Support for application policies on per-group basis
  - Enhanced Integration with PocketCloud Remote Desktop Pro app (iOS and Android)
  - Support for assigning multiple roles to single user
  - Support for Republish Policies options for mobile devices
  - Support for deleting inactive users and devices from system
  - Enhancements for tracking policy/application changes

- **New Features Details**

  The new functionality described below is presented in order of tab view: Groups / Users / Devices / Events / Portal Admin (new).

1. **Groups Tab**
   - **Thin Client policy changes**:

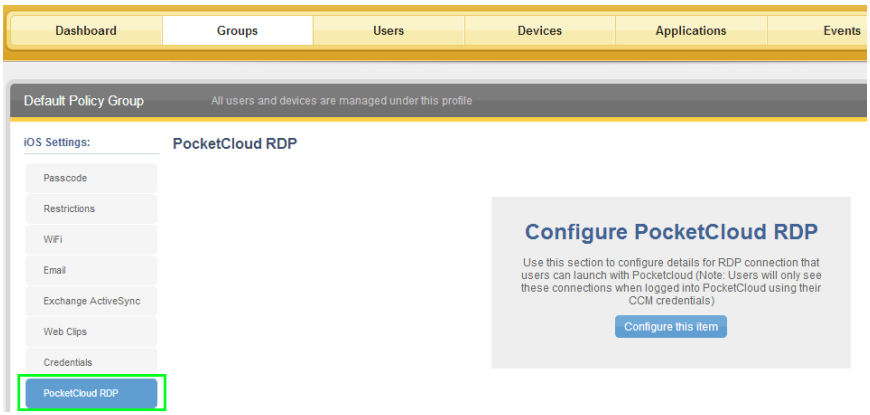


     - **Display**: "Default Wallpaper color" option removed
     - **Visual Experience**: New Zero Launchpad settings:
       i. Enable Zero toolbar activation in left margin:
          1. On Mouseover after ____ seconds
          2. Only after clicking
       ii. Number of seconds before toolbar is activated
       iii. Disable Hotkey (CTRL-ALT-UP) to show toolbar
       iv. Always disable toolbar when only have 1 session available
       v. Disable Home Icon

- **Security**:
    i. New settings:
        1. Enable Gkey reset
        2. Enable Trace
        3. Enable VNC
            a. VNC Password
            b. Prompt User on start
            c. Counter for Accept/Reject
            d. Prompt User on end
            e. View Only
            f. Force 8bit

- **Remote Connections**:
    i. If Broker=”None”, “Microsoft”, “Vmware”:
        1. New Settings:
            a. Enable NLA
            b. Enable Recording
            c. Force Span
            d. Enable Desktop Wallpaper
            e. Enable Window Dragging
            f. Enable Animation
            g. Enable Theme
    ii. If Broker=”Citrix”:
        1. New settings:
            a. USBRedirection Technology: (TCX, HDX)
            b. Enable Session Reliability
            c. Enable Progressive Display
            d. Display on desktop: (None, Apps Only, Apps & Desktop)
            e. Enable Branch Repeater
            f. Enable ICA Ping
            g. AudioQuality: (Default, Low, Medium, High)
            h. Map USB disks to: (No Mapping, A, B, ..., Y, Z)
- **Central Configuration**:
    i. New Option: Firmware Update Logic (Do not update, New firmware only, Any different firmware)
        1. If “New firmware only” or “Any different firmware”, new option: “Local Prompt”
- **Other**: No changes
- **Advanced**: No changes

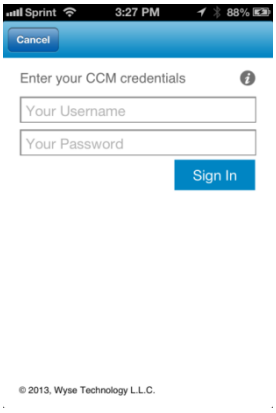
- **PocketCloud RDP policy changes** (iOS & Android):
  - **Note*: PocketCloud RDP only available with PRO Tier***



  - "**PocketCloud**" button removed from CCM Agent (iOS and Android). Users are now able to login with Cloud Client Manager credentials directly from ***PocketCloud Remote Desktop Pro*** app (iOS and Android) to access corporate connections configured from Cloud Client Manager.

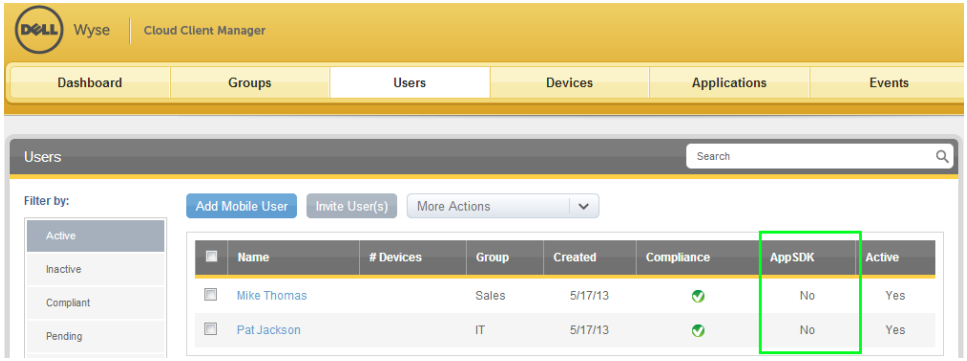
    In ***PocketCloud Remote Desktop Pro*** app there is a new "CCM" section. Click "**Sign In**", enter the CCM user credentials and the corporate connections configured in Cloud Client Manager will now appear in the "**My Computers**" list in the "**CCM Connections**" section.

Sprint 3:27 PM 88%
Settings
Auto Discovery
Username: wyse200@g...
Sign Out
Signing in using your Gmail credentials means hassle-free access to your devices with minimal setup, and no technical know-how needed.
CCM
Setup your CCM login
Sign In
Signing in using your CCM credentials means that you will need access from your Admin IT
PocketCloud Premium
My Computers
Settings
Help
File Transfers

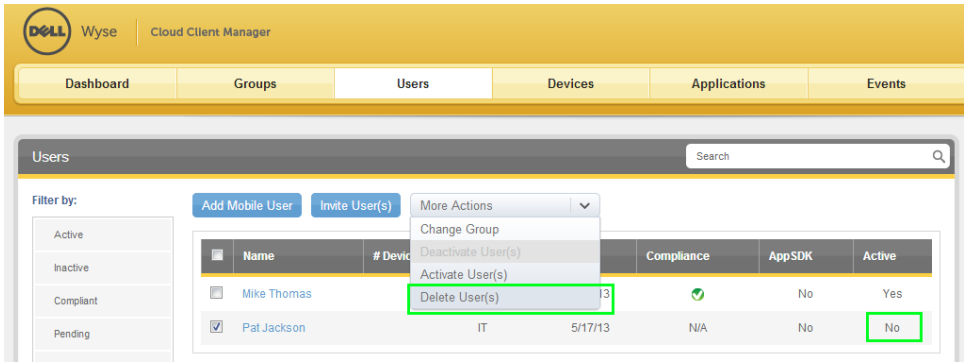


2. Users Tab

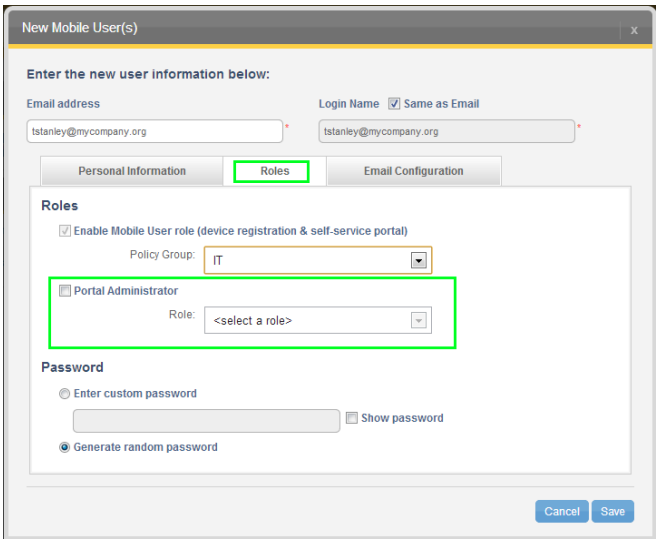
- New column in main Users table: “AppSDK” - set to “Yes” for users that have logged into ***PocketCloud Remote Desktop Pro*** app using Cloud Client Manager credentials



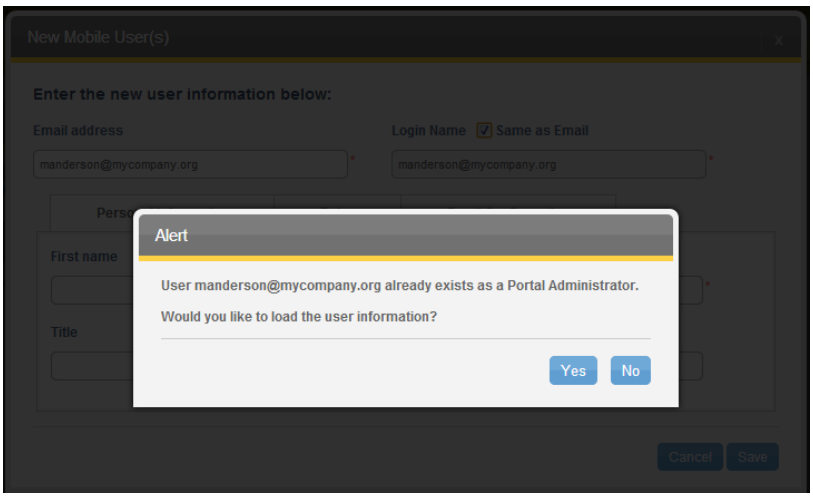
- New option on users: “**More Actions > Delete User(s)**” (NOTE: user must be deactivated prior to deleting)



- Reorganization of “New Mobile User” dialog:
  - Add “Portal Administrator” role while adding user: when adding users from **Users** page can also provide one of the Cloud Client Manager administrator roles (Global Administrator; Global Viewer).

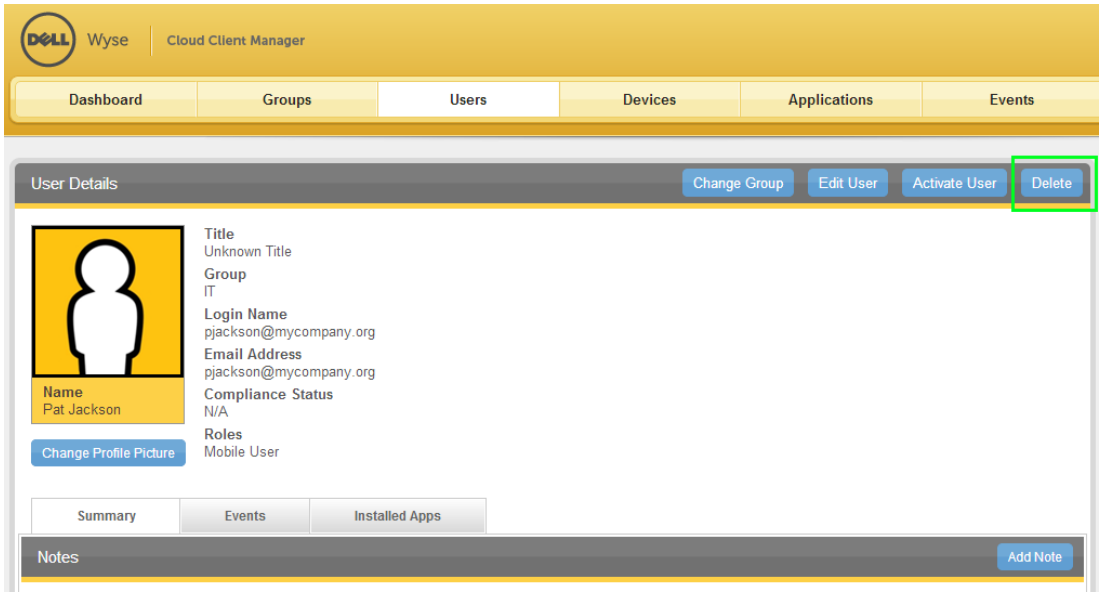


- Detection for matching Login Name with current Portal Administrators – if user exists with same Login Name prompt if user wants to add Mobile User role to existing use account (all configured user information will be automatically populated)

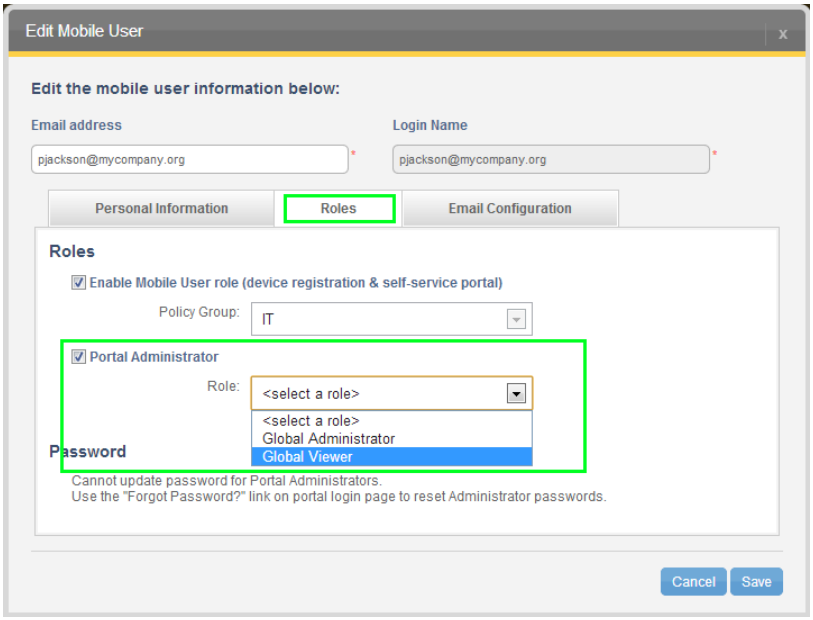


3. Users Details View

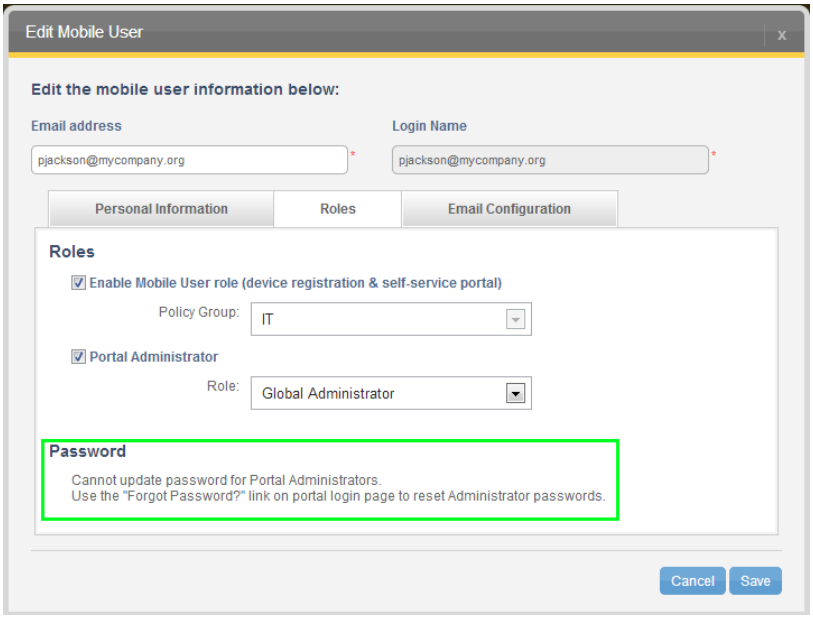
- New option: "**Delete**" (users must be deactivated prior to deleting)



- Reorganization of "Edit Mobile User" dialog:
  - Add "Portal Administrator" role on existing user: when editing users from Users page can also provide one of the Cloud Client Manager administrator roles (Global Administrator; Global Viewer).

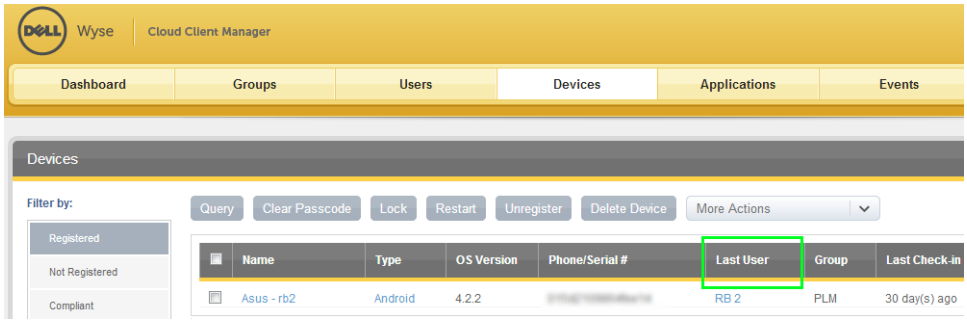


- Change Password: cannot update a user password if user has a Portal Administrator role (must use "**Forgot Password**" link on Cloud Client Manager sign-in page)

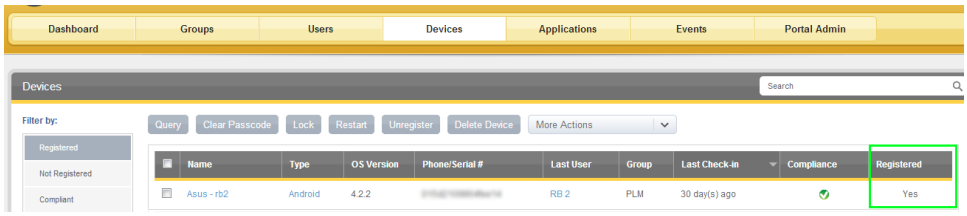


4. Devices Tab

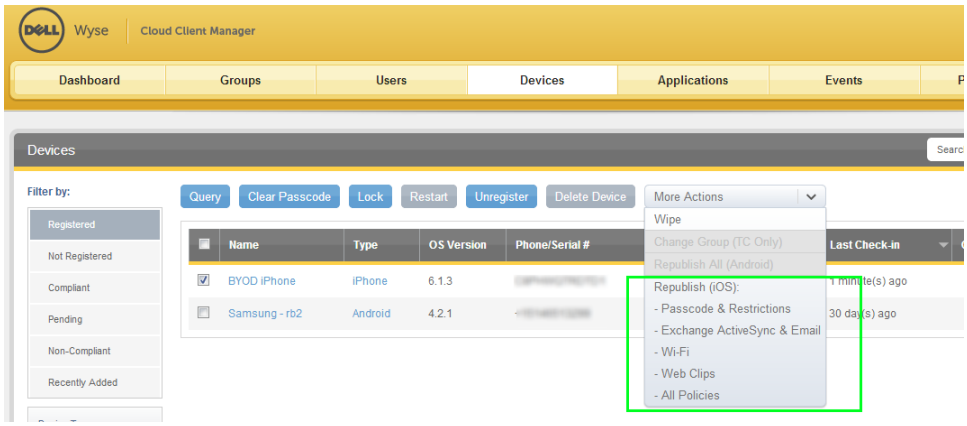
- Rename column in main Devices table: “User Name” -> “Last User”



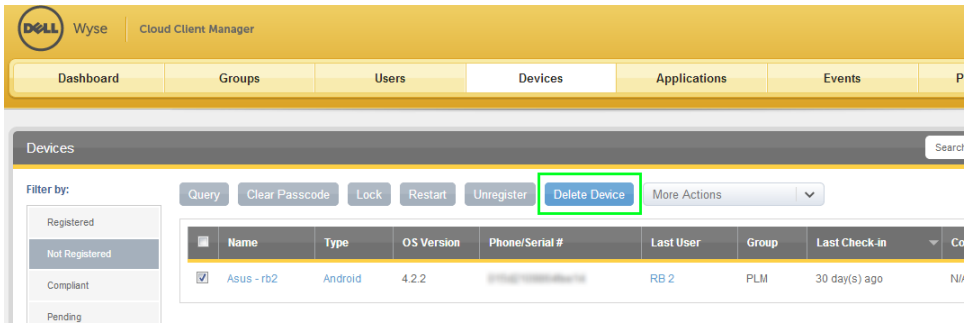
- Rename column in main Devices table: “Active” -> “Registered”



- New option on devices: “**More Actions > Republish**”:
  - **Republish All (Android)**: Republishes all policies applied to selected Android device
  - **Republish (iOS)**: For selected iOS devices, republishes specific policies below or “All” policies assigned to device: Passcode & Restrictions; Exchange ActiveSync & Email; Wi-Fi; Web Clips; All Policies

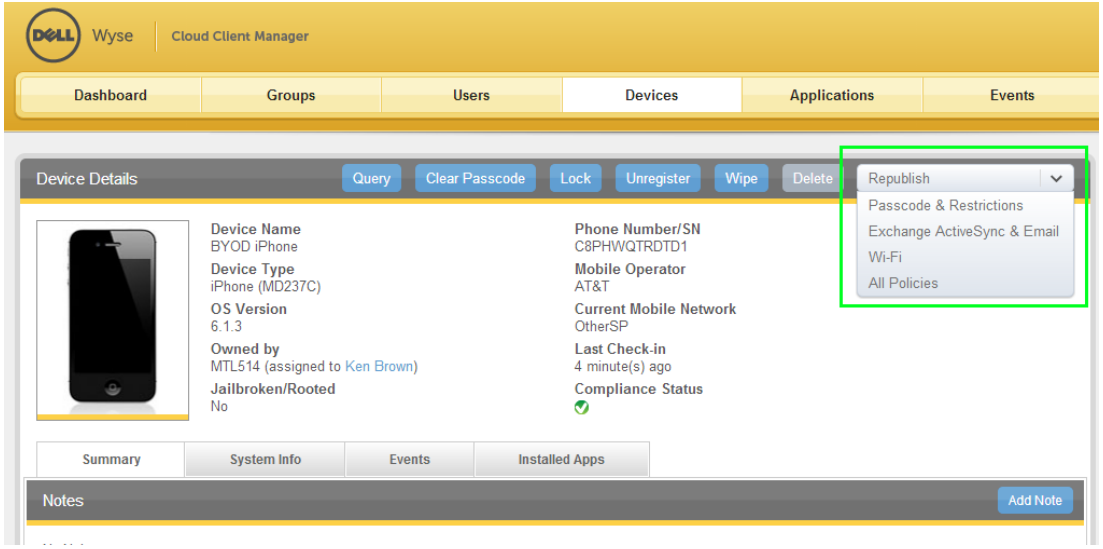


- New option on devices: “**Delete Device**” to remove from system (device must be deactivated)

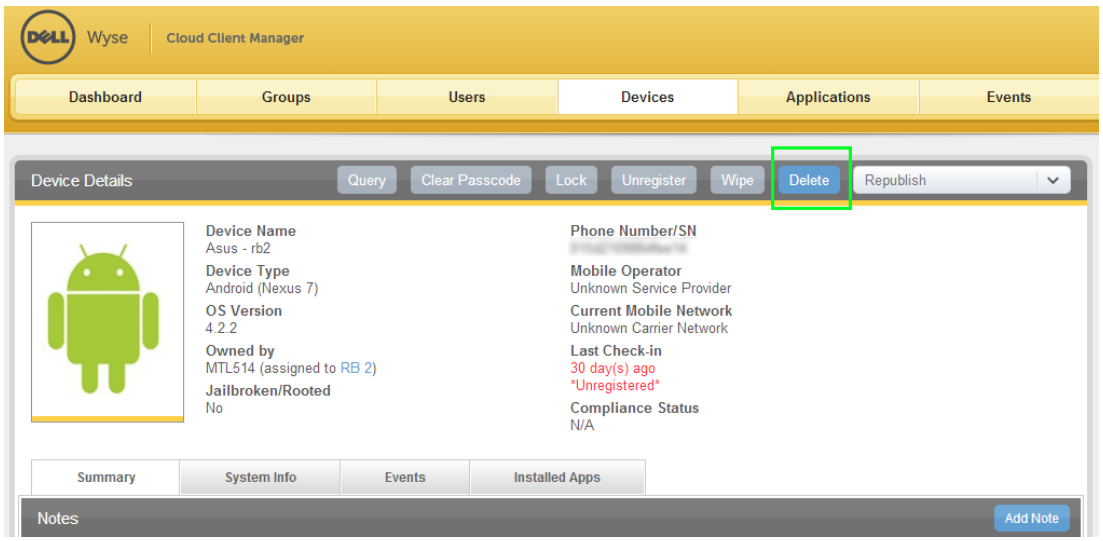


5. Device Details View

- New “Republish” options to republish the assigned policies for device:
  - Republish All (Android): Republishes all policies applied to selected Android device
  - Republish (iOS): for selected iOS devices, republishes specific policies below or “All” policies assigned to device:
    - Passcode & Restrictions
    - Exchange ActiveSync & Email
    - Wi-Fi
    - Web Clips
    - All Policies

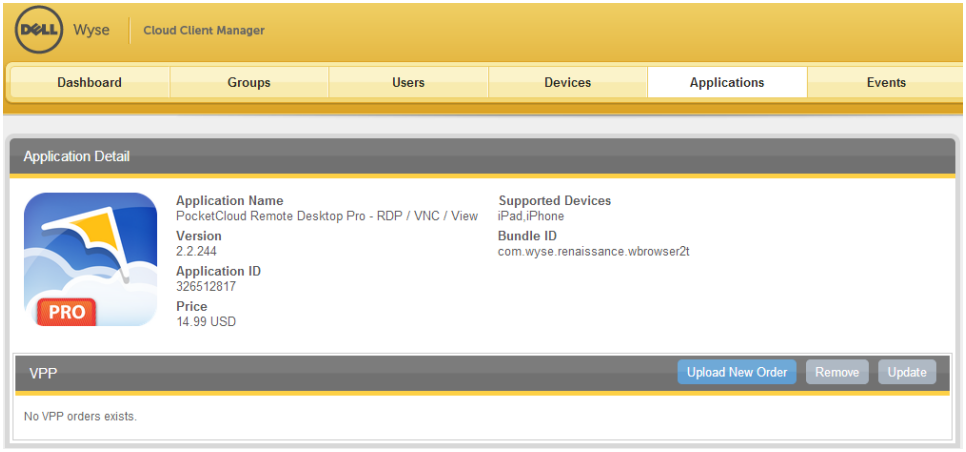


- New “Delete” option: for devices that are unregistered, option to delete the device from system

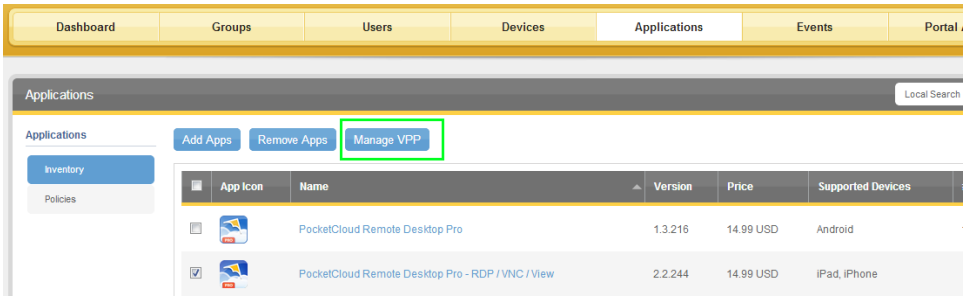


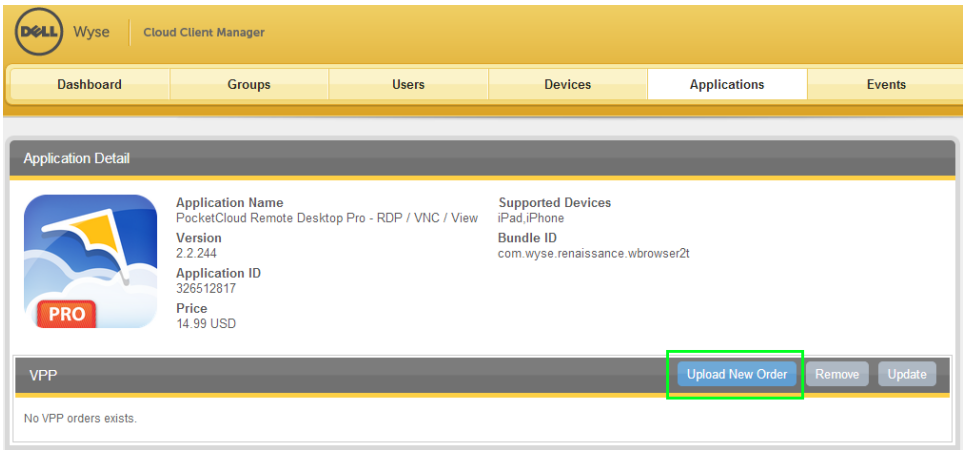
6. Applications tab

- ***App Management only available with PRO Tier***
- Application Inventory:
  - Clicking on App Name now brings **Application Details** view which provides further details of app

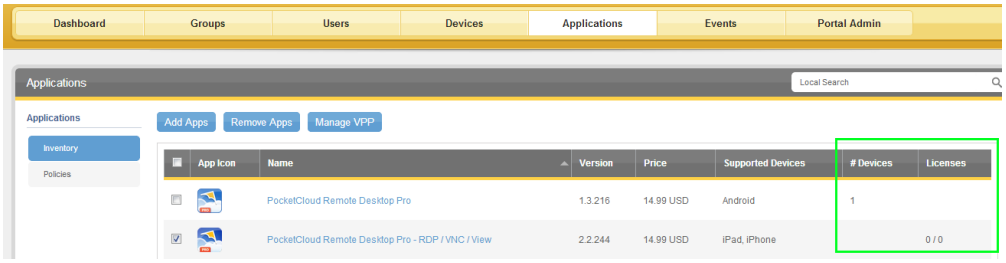


  - New "**Manage VPP**" option (brings user to **App Details** view): Manage iOS VPP spreadsheets for purchase orders made from Apple VPP store. Allows for enterprises to push out paid applications to iOS devices, and monitor the number of total and redeemed licenses (tied to redemption codes). Use the "**Upload New Order**" button to import Apple VPP licenses from spreadsheet.

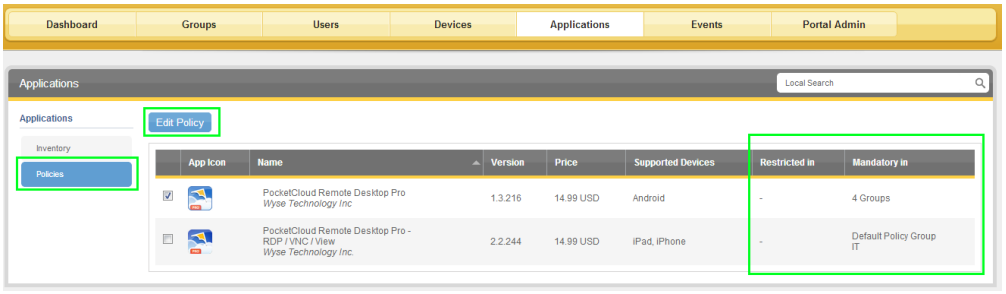


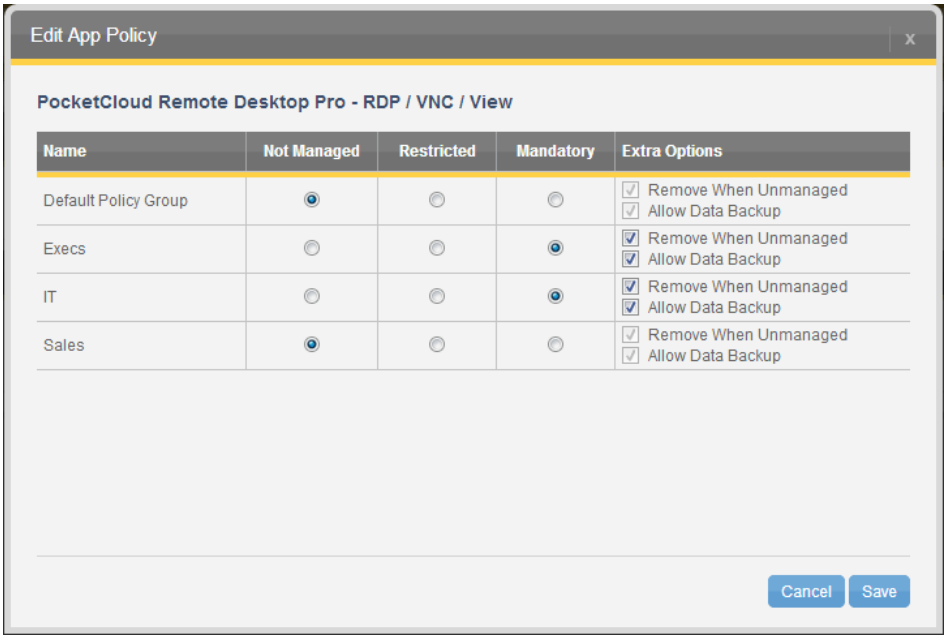


- Updated layout:
  - # **Devices**: number of devices with application installed
  - **Licenses**: Shows number of VPP license redemption codes redeemed and total number of redemption codes uploaded per paid iOS app



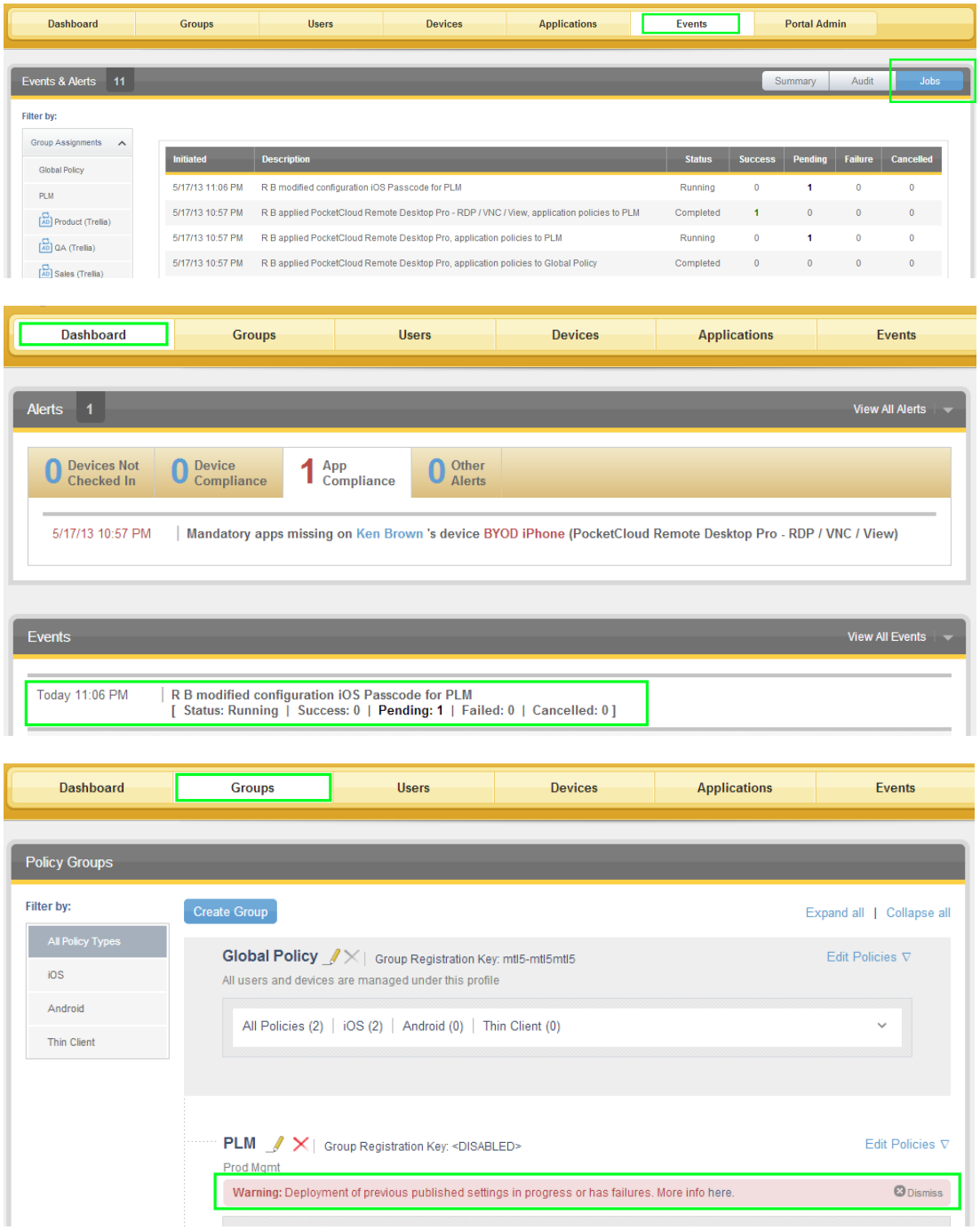
- Application Policies:
  - Updated layout: Provides further details on application in the main **Policies** page in addition to a summary of which Policy Groups have the app tagged as either “Restricted” or “Mandatory”
  - New “**Edit Policy**” option: can now assign app policies on a per-group basis (Not Managed, Restricted, Mandatory)





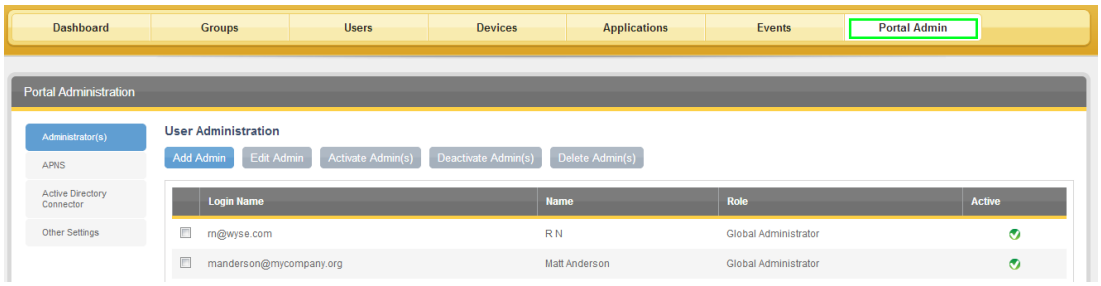
7. Events Tab

- New “Jobs” tab: Jobs are a new concept in this release. For policy or application policy changes at the Group level this will create a corresponding Job that will track status for all devices affected by change: Success/Pending/Failure/Cancelled. Can also click the device count under the Status to view more details regarding the Job. Jobs can also be viewed from **Dashboard > Events** and in the **Groups** tab for any job that is still ongoing or if any action failed with link to job details.

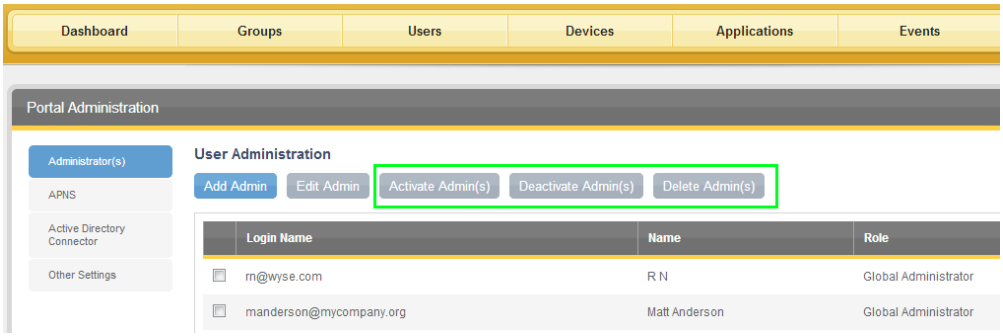


8. Portal Admin Tab

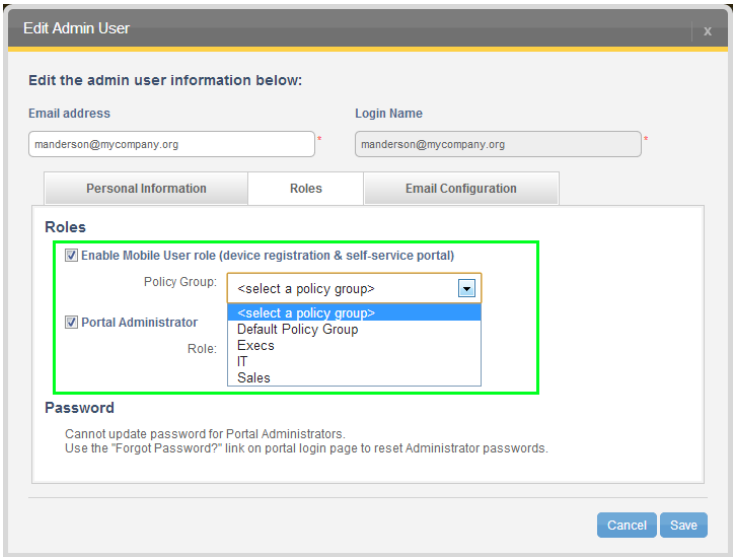
- New **"Portal Admin**" tab (in previously options were available from *Administrator(s) / APNS / Self-Service* views accessible from clicking on the logged in username at top-right of screen)



- **Administrators** menu:
  - Changes to menu options:
    - Rename options: "Enable Admin" > "Activate Admin(s)"; "Disable Admin" > "Deactivate Admin(s)"
    - New Option: "**Delete Admin(s)**" (Note: user must be deactivated to be deleted)

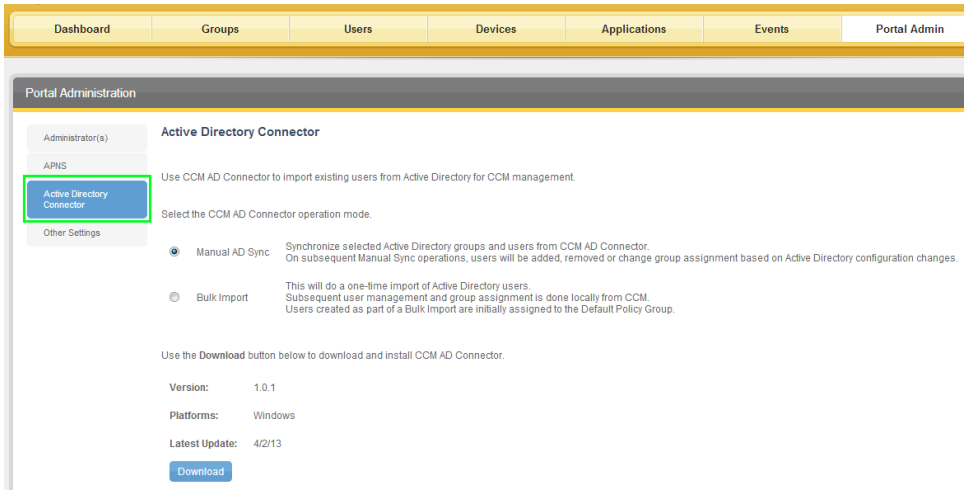


  - Administrators can now also have "Mobile User" role (during Add and Edit)

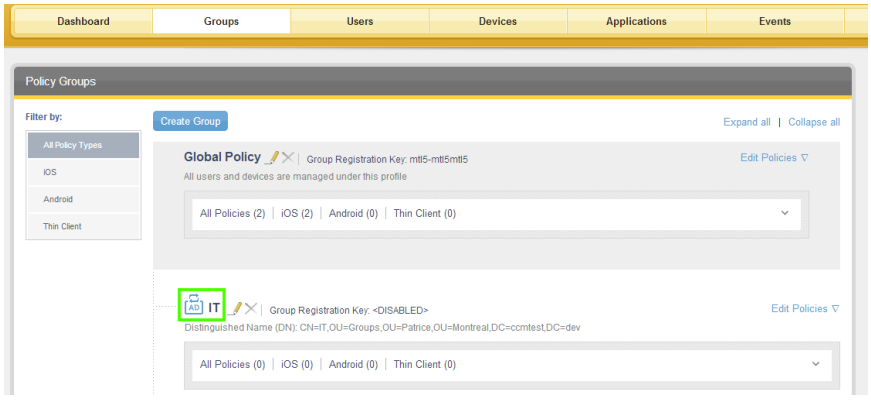


- **APNS** menu: now accessible from **Portal Admin** tab

- **Active Directory Connector** menu:
  - ***AD Integration only available with PRO Tier***
  - Active Directory Integration allows for users to be imported from Active Directory with option to manage users locally or ongoing according to AD account status and AD group assignment. Requires use of **CCM AD Connector** app – downloadable from Cloud Client Manager portal
  - Two Modes of Operation
    1. **Bulk Import**: This will do a one-time import of Active Directory users. Subsequent user management and group assignment is done locally from CCM. Users created as part of a Bulk Import are initially assigned to the Default Policy Group.
    2. **Manual AD Sync**: Synchronize selected Active Directory groups and users from CCM AD Connector. On subsequent Manual Sync operations (using **CCM AD Connector** application), users will be added, removed or change group assignment based on Active Directory configuration changes

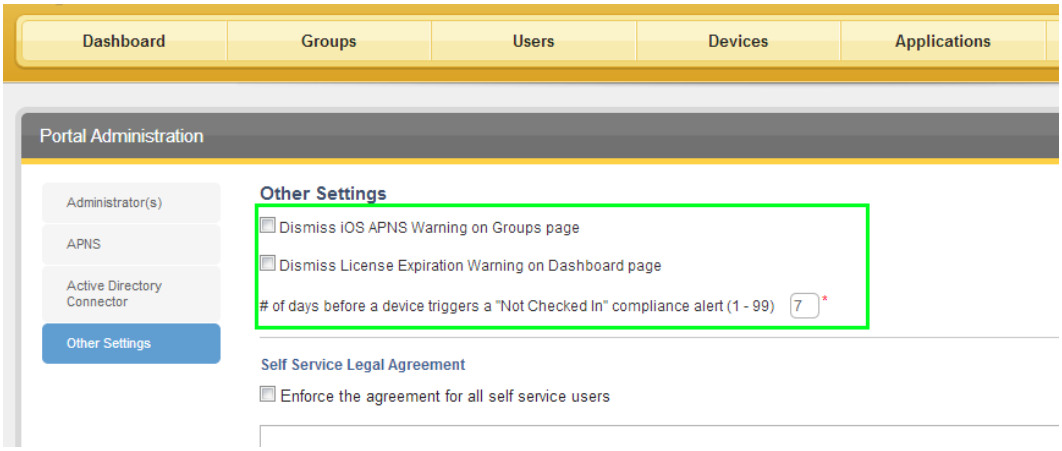

Dashboard
Groups
Users
Devices
Applications
Events
Portal Admin
Portal Administration
Administrator(s)
APNS
Active Directory Connector
Other Settings
Active Directory Connector
Use CCM AD Connector to import existing users from Active Directory for CCM management.
Select the CCM AD Connector operation mode.
Manual AD Sync
Synchronize selected Active Directory groups and users from CCM AD Connector.
On subsequent Manual Sync operations, users will be added, removed or change group assignment based on Active Directory configuration changes.
Bulk Import
This will do a one-time import of Active Directory users.
Subsequent user management and group assignment is done locally from CCM.
Users created as part of a Bulk Import are initially assigned to the Default Policy Group.
Use the Download button below to download and install CCM AD Connector.
Version: 1.0.1
Platforms: Windows
Latest Update: 4/2/13
Download

  - AD Group Indicator: For groups added as part of a Manual AD Sync an AD icon appears next to the group name.



  - Refer to the Cloud Client Manager support site for further details on configuring AD Integration: https://support.cloudclientmanager.com/entries/23859461-Cloud-Client-Manager-Active-Directory-Integration-Overview

- **Self-Service** menu:
  - Menu renamed to "**Other Settings**"
  - New Option: "**Dismiss iOS APNS Warning on Groups page**" which will remove the warning that appears in the group page when no iOS APNS certificate has been uploaded (from **Portal Admin > APNS**)
  - New Option: "**Dismiss License Expiration Warning on Dashboard page**" which disable warnings for license expiration from appearing on the Dashboard page
  - New Option: **"# of days before a device triggers a "Not Checked In" compliance alert (1 - 99)"** to configures number of days that a device must do a Check-In by to avoid being tagged as "Not Compliant".



Supported Devices

Thin Client Requirements

- **Supported Devices:** Thin Clients supported include:
  - C00X (Wyse Xenith) running firmware 2.0_021 or later (recommended 2.0_026 or later)
  - R00LX (Wyse Xenith Pro) running firmware 2.0_021 or later (recommended 2.0_026 or later)
  - T00X (Xenith 2) running firmware 2.0_021 or later (recommended 2.0_026 or later)
  - C10LE running firmware ThinOS 7.1_207 or later
  - R10L running firmware ThinOS 7.1_207 or later
  - T10 running firmware ThinOS 7.1_207 or later

  For supported thin clients running earlier versions, a firmware update is required to enable Cloud Client Manager connectivity. Updates can be downloaded from the Wyse Self-Service Center at: http://support.wyse.com/selfservice.html

  IMPORTANT: You must use your *ThinOS Maintenance* (you should have received an email from Wyse or your reseller with full instructions) to obtain available firmware updates (if you did not receive this email, contact your reseller). If unfamiliar with updating firmware on Wyse ThinOS cloud clients, refer to Wyse Knowledge Base Solution #**10566** (go to Wyse Knowledge Base at http://www.wyse.com/kb and search for **10566**).

- **Connectivity Requirements:**
  - TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com

iOS Requirements

- **Supported Devices:**
  - iPhone and iPad running iOS Version 5.x and later
- **Connectivity Requirements:**
  - TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 80 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 8443 (outbound) to us1-mdm.cloudclientmanager.com
  - TCP port 5223 (outbound) - for Apple APNS
- **MDM Certificate Requirements:**
  - A Mobile Device Management (MDM) Apple Push Notification Service (APNs) certificate is required for iOS device management - this process requires an Apple ID. As the Apple ID account will be linked to the APNs certificate, which must be renewed annually, a corporate Apple ID account should be used and not a personal one

Android Requirements

- **Supported Devices:**
  - Devices running Android Version 2.3 and later
- **Connectivity Requirements:**
  - TCP port 443 (outbound) to https://us1.cloudclientmanager.com
  - TCP port 1883 (outbound) to us1-pns.cloudclientmanager.com

Upgrade Notes

It is recommended to upgrade to the latest mobile device agents for this release of Cloud Client Manager:

- **iOS** - The latest Cloud Client Manager Agent update for iOS is available from the App Store: https://itunes.apple.com/app/cloud-client-manager-agent/id567787460?mt=8
- **Android** - The latest Cloud Client Manager Agent update for Android is available from the Play Store:https://play.google.com/store/apps/details?id=com.wyse.ccm.android&hl=en

- **Known Issues**

STR-678	iOS registration fails if re-registering within 30 seconds
STR-842	Some iOS/Android sub-options at lower policy level not affected by changes to parent options at higher policy level
STR-1148	Android device prompts for app install for installed System apps
STR-1173	Remove certificate for iOS payload fails unless linked payload is removed
STR-1409	Picture taken from the Android back camera compressed on Agent display (correct on server)
STR-1497	iOS Webclip uploaded image truncated in IE8 in CCM console
STR-2335	User/Device Details summary view not displaying some iOS settings when payload configured at higher level is saved with default settings at user/device level.
STR-2356	Formatting issues in app policy UI for policy groups with long group names
STR-2414	Event missing when removing device-level exception payloads
STR-2449	Cannot deactivate AD user missing required user information
STR-2489	Apps installed from App Store not tagged as “not managed” in CCM Agent when user cancels the app install request on device
STR-2552	VPP file name is not cleared if upload is cancelled and reinitiated
STR-2613	Feedback missing on iOS Agent when trying to initiate paid app install and no redemption code available
STR-2675	Some Thin Client CCM policies override policies set in Global .ini
STR-2712	Some Android devices displaying app identifier instead of app name in Restrictions message
STR-2726	Extra remove profile command generated when assigning two payloads for same policy type at different policy levels
STR-2786	Changing Android app policy multiple times between mandatory to not managed may cause extra remove application commands
STR-2922	Changing Android policy sometimes requires Republish to push policies
STR-3030	Application missing from Installed Apps list for iOS and Android applications with same bundle/application identifier
STR-3031	Registered thin client does not go to “Pending” status after group change (delete group action)
STR-3033	Layout issues with IE “Compatibility View” feature enabled
CCMPC-137	Passcode policy not removed from device when restriction applied at lower level and passcode applied/removed at default policy group level